

Alexander Mahnke
Torsten Rohlfs *Hrsg.*

Betriebliches Risikomanagement und Industriever sicherung

Erfolgreiche Unternehmenssteuerung
durch ein effektives Risiko- und
Versicherungsmanagement



Springer Gabler

Betriebliches Risikomanagement und Industriever sicherung

Alexander Mahnke • Torsten Rohlf
Hrsg.

Betriebliches Risikomanagement und Industriever sicherung

Erfolgreiche Unternehmenssteuerung
durch ein effektives Risiko- und
Versicherungsmanagement



Springer Gabler

Hrsg.

Alexander Mahnke
Siemens AG
München, Deutschland

Torsten Rohlf
TH Köln, Institut für Versicherungswesen
Köln, Deutschland

ISBN 978-3-658-30420-1

ISBN 978-3-658-30421-8 (eBook)

<https://doi.org/10.1007/978-3-658-30421-8>

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Springer Gabler

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von allgemein beschreibenden Bezeichnungen, Marken, Unternehmensnamen etc. in diesem Werk bedeutet nicht, dass diese frei durch jedermann benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des jeweiligen Zeicheninhabers sind zu beachten.

Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag, noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Springer Gabler ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.

Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Vorwort

Die vorliegende Ausarbeitung ist im Rahmen eines gemeinsamen Forschungsprojektes des Gesamtverbands der versicherungsnehmenden Wirtschaft e. V. (GVNW) und des Instituts für Versicherungswesen (IVW) an der Technischen Hochschule Köln entstanden. Die Studierenden des (auch international ausgerichteten) Studiengangs „Master of Risk & Insurance“ des IVW haben dazu zusammen mit ausgewählten Vertretern des Industriever sicherungsmarktes an spezifischen Fragestellungen aus den Bereichen Risikomanagement und Industriever sicherung gearbeitet.

Ziel des Projektes war es, ein vertieftes und praxisorientiertes Verständnis für das industrielle Risikomanagement zu entwickeln und strukturiert für interessierte Studenten und Praktiker aufzubereiten. In den verschiedenen Beiträgen werden hierzu der Risikomanagementprozess ausführlich dargestellt, auf verschiedene Aspekte des unternehmerischen Risikomanagements eingegangen, der Industriever sicherungsmarkt vorgestellt und ausgewählte Unternehmensrisiken mit möglichen Versicherungslösungen diskutiert. Die Ausarbeitungen geben dabei ausschließlich Meinung und Standpunkt der Autoren wieder.

Dieses Projekt hätte nicht entstehen können ohne die tatkräftige Unterstützung vieler Seiten. Unser herzlicher Dank gilt zunächst allen Studierenden und Praxisvertretern, die uns mit ihren Beiträgen einen Einblick in die Praxis des Risikomanagements und der Industriever sicherung geben. Darüber hinaus bedanken wir uns bei den beiden Geschäftsführern des GVNw, Herrn Jörg F. Henne und Herrn Reiner Siebert, die uns bei der Suche nach Autoren und bei der Koordination im gesamten Projektlauf tatkräftig unterstützt haben. Schließlich bedanken wir uns auch bei dem sehr engagierten studentischen Projekt leitungsteam, Frau Katharina Faßbender und Herrn Philipp Nießen, welche das Projekt auf Seiten des IVW koordiniert haben.

Wir wünschen allen Lesern eine interessante Lektüre mit vielen Anregungen für den praktischen Alltag.

Bonn, Deutschland
Köln, Deutschland

Dr. Alexander Mahnke
Prof. Dr. Torsten Rohlf

Inhaltsverzeichnis

Teil I Einführung

1 Risikomanagement im Unternehmen	3
Torsten Rohlfs und Alexander Mahnke	

Teil II Risikomanagementprozess

2 Risikoidentifizierung und -klassifizierung	19
Wolfgang Knauf und Jessica Bender	
3 Risikoanalyse, -bewertung und -steuerung.....	41
Alexander Skorna und Philipp Nießen	
4 Effektive Risikokultur: Bedeutsam für Organisation, Kontrolle und Kommunikation von Risiken	67
Benedikt Hintze und Philipp Beuker	

Teil III Betriebliches Risikomanagement

5 Klassische Risiken im Überblick	89
Daniel Aschoff und Julian Heitmann	
6 Emerging Risks	115
Jörg F. Henne und Leonard Wenzel	
7 Risiko- und Versicherungsmanagement	135
Detlef Hesse und Fabio Papa	
8 Technisches Risikomanagement	147
Thomas Bär und Yannick Berkemeier	
9 Schaden- und Krisenmanagement	169
Michael Seidl und Kathrin Regeling	
10 Business Continuity Management.....	191
Marco Mirkes und Emine Özcan	

11	Zertifizierung von Risikomanagementsystemen und -prozessen	213
	Olaf Seiche und Erik Klaedtke	
12	Corporate Governance und Compliance	235
	Andreas Biegel und Pascal Müller	
13	Digitalisierung & Risikomanagement	255
	Markus Vorbringer und Thorben Schlätzer	

Teil IV Der Industrieverversicherungsmarkt

14	Versicherungsnehmer und Firmenverbundener Vermittler	277
	Jörg Maier und Katharina Faßbender	
15	Bedeutung und Zukunft des Industrieverversicherungsmaklers in Deutschland	297
	Mathias Pahl, Mirko Domazet und Juliane Ressel	
16	Industrieverversicherer im Marktumfeld der Industrieverversicherung	319
	Christopher Lohmann, Stefan Sowitzki und Pauline Gewand	
17	Captives	355
	Holger Kraus und Julian Alexander Robles Häusser	
18	Rolle des Rückversicherers in der Industrieverversicherung	375
	Angelika Trotta und Jan Fischer	
19	Alternativer Risikotransfer	399
	Ralf Weyand und Mathis Herzke	

Teil V Risiken, Risikomanagement und Versicherungsaspekte

20	Internationale Versicherungsprogramme	429
	Rüdiger Auras und Michael Dehm	
21	Cyber	447
	Andreas Walz, Jörg Klemens und Romina Röpke	
22	Warranty & Indemnity-Versicherung bei der Unternehmenstransaktion	471
	Carolin van Straelen, Bernd Dreier und Jannik Revers	
23	Betriebs- und Produkthaftpflichtversicherung	485
	Georg Klinkhammer und Harald Kurtze	
24	Financial Lines – D&O-Versicherung	505
	Marcel Wilms und Christopher Schatz	
25	Risikomanagement in der Supply-Chain	531
	Christian Müller und Jan Tschöpe	

26	Produktrückruf und Produkthaftung, Qualitätssicherung	557
	Christian Kuhrt und Monique Neußmann	
27	Naturgefahren	581
	Malwine Tewes und Andrea Scholtes	
28	Transport und Warenkredit	601
	Reiner Siebert und Lukas Spohr	
29	Terror- und politische Risiken	625
	Leo Zagel, Volker Steinmetz und Hans Lange	
30	Travel Risk Management	645
	Martin Gary und Tim Thomas	
31	Betriebliche Altersversorgung	667
	Ingo Trosiner und Dominik Hartmann	
32	Projektmanagement und Projektversicherung	689
	Lutz Torbohm und Svenja Schröder	
33	Rating und Solvency II	709
	Hüseyin Kaya und Mergime Rahimi	
34	Herausforderungen bei der Schadenregulierung	737
	Birgit Beudt und Frank Cremer	

Teil I

Einführung



Risikomanagement im Unternehmen

1

Torsten Rohlfs und Alexander Mahnke

Zusammenfassung

Aus der heutigen Perspektive kann Risikomanagement als Gesamtheit aller Maßnahmen nur durch eine unternehmensweite, ganzheitliche und antizipative Betrachtung sämtlicher Risiken in einem bereichsübergreifenden Prozess sinnvoll und effektiv betrieben werden. Die Risiken werden nicht mehr isoliert betrachtet, sondern werden im Unternehmenskontext global analysiert. Der mit dieser Zielsetzung ausgerichtete Risikomanagementprozess wird auch als Enterprise Risk Management bezeichnet.

1.1 Enterprise Risk Management

Unternehmen agieren unter **Unsicherheit**. Die zentrale Herausforderung für das Management besteht darin, zu entscheiden, wie groß die Unsicherheit im Rahmen der unternehmerischen Tätigkeit werden darf bzw. wie viel Risiko das Unternehmen bereit ist einzugehen.

Somit kann auch der unternehmerische Erfolg nicht ohne das eingegangene Risiko betrachtet werden. Über eine **wert- und risikoorientierte Steuerung** sollen gerade Geschäftsstrategie und eingegangene Risiken als Mehrwert-Betrachtung verbunden werden. Aus Sicht der Unternehmenssteuerung sind die Geschäfts- und Risikostrategie gemeinsam abzubilden und zu beurteilen. Die aus den Unternehmenszielen abgeleiteten Geschäfts-

T. Rohlfs (✉)

TH Köln, Institut für Versicherungswesen, Köln, Deutschland

E-Mail: torsten.rohlfs@th-koeln.de

A. Mahnke

Siemens AG, München, Deutschland

E-Mail: mahnke.alexander@siemens.com

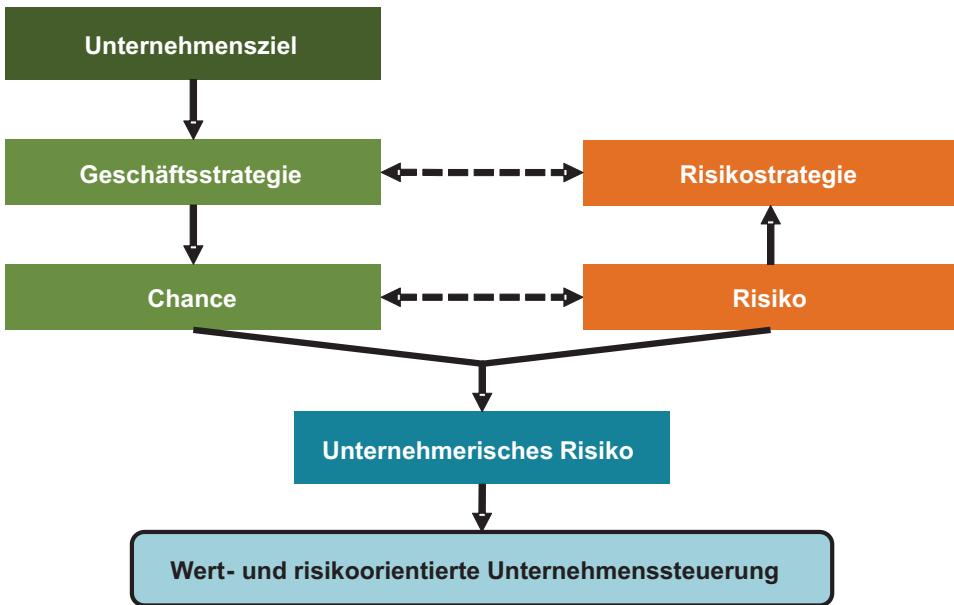


Abb. 1.1 Unternehmenssteuerung. (Quelle: eigene Darstellung in Anlehnung an Rohlfs et al. 2019, S. 18)

strategien werden nicht isoliert festgelegt, sondern immer im Kontext mit dem eingegangenen Risiko beurteilt (vgl. Abb. 1.1; vgl. hierzu Rohlfs et al. 2019, S. 17 ff.).

Ausgangspunkt sind die von der Geschäftsführung formulierten zentralen **Unternehmensziele** als definiertes Ambitionsniveau im Hinblick auf

- Gewinn,
- Wachstum,
- Sicherheit und
- Steigerung des Unternehmenswertes.

Die so vorgegebenen Unternehmensziele werden über eine Gesamtplanung mit aufeinander aufbauenden Teilplänen als konkrete Geschäftsstrategie umgesetzt.

Da die **Geschäftsstrategie** unter Unsicherheit bestimmt wird, sind die ausgearbeiteten Maßnahmen und entsprechenden Chancen mit Geschäftsrisiken verbunden. Diese strategiebezogenen Risiken wiederum bedrohen die ursprünglich der Geschäftsstrategie zugrunde gelegten Unternehmensziele. Durch das direkte Zusammenspiel von Unternehmenszielen, Geschäftsstrategien und Geschäftsrisiko sind daher **Risikostrategie** und Geschäftsstrategie eng miteinander verzahnt. Beide sind Bestandteil der strategischen Unternehmenspolitik.

Die Wechselwirkung von Geschäfts- und Risikostrategie beschreibt das **unternehmerische Risiko** (spekulatives Risiko). In Unternehmen sollte daher ein starkes Bewusstsein (Risikokultur) dafür herrschen, dass Risiken im Rahmen der eigenen Geschäftstätigkeit bestehen, welche das Erreichen von Unternehmenszielen und Geschäftsstrategien erschweren können. Dies ist auch im Interesse der im Unternehmen handelnden Leitungs- und Aufsichts-

organe (Vorstände, Geschäftsführer, Aufsichtsräte etc.), da sie ggf. für die Folgen ihrer Tätigkeiten gegenüber dem Unternehmen (und im Ausnahmefall Dritten gegenüber) haften können.

Dies ist so auch in der **Gesetzgebung** verankert. Der Vorstand einer Aktiengesellschaft hat gemäß § 76 Abs. 1 AktG unter eigener Verantwortung die Gesellschaft zu leiten. Im Hinblick auf das Risikomanagement gibt es im deutschen Aktiengesetz (AktG) zwei wichtige Regelungen:

Nach § 91 Abs. 2 AktG (eingeführt im Jahre 1998 durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich, KonTraG) hat der Vorstand ein Risikofrüherkennungssystem für solche Risiken einzurichten, die den Fortbestand der Gesellschaft gefährden. Auch wenn es vordergründig um das Analysieren bestandsgefährdender (also extremer) Risiken geht, verankert dies ein Risikomanagementsystem in der Geschäftsorganisation. Denn folgerichtig muss dann auch der Umgang mit diesen Risiken geklärt werden. Ebenso müssen identifiziert „wesentliche“ (aber nicht bestandsgefährdende) Risiken weiter analysiert und behandelt werden, auch wenn sie dem Wortlaut nach nicht unter das Risikofrüherkennungssystem fallen.

§ 93 Abs. 1 S. 1 AktG regelt, dass die Vorstandsmitglieder bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden haben (§ 43 Abs. 1 GmbHG enthält eine nahezu wortgleiche Regelung). Tun sie dies nicht, so haften sie nach § 93 Abs. 2 S. 1 AktG für den daraus entstehenden Schaden (hierzu ausführlich Lange, D&O-Versicherung und Managerhaftung, § 2). Dies zwingt den Vorstand unter anderem dazu, im Rahmen der Unternehmenssteuerung ein funktionierendes Risikomanagement zu implementieren. Dabei ist allerdings zu berücksichtigen, dass eine die Haftung auslösende Pflichtverletzung dann nicht vorliegt, „wenn das Vorstandsmitglied bei einer unternehmerischen Entscheidung vernünftigerweise annehmen durfte, auf der Grundlage angemessener Information zum Wohle der Gesellschaft zu handeln“ (§ 93 Abs. 1 S. 2 AktG). Diese, nach US-amerikanischem Vorbild konzipierte sogenannte „Business Judgement Rule“ gilt entsprechend für Geschäftsleiter anderer Unternehmen, wie zum Beispiel der GmbH (vgl. hierzu Lange, D&O-Versicherung und Managerhaftung, § 2, Rn. 48 m. w. N.).

Betrachtet man das Zusammenspiel von Geschäftsstrategien und Geschäftsrisiken, benötigt man im Unternehmen Prozesse, die die Geschäftsrisiken entsprechend steuern können (Prozesssicht) (vgl. Abb. 1.2).

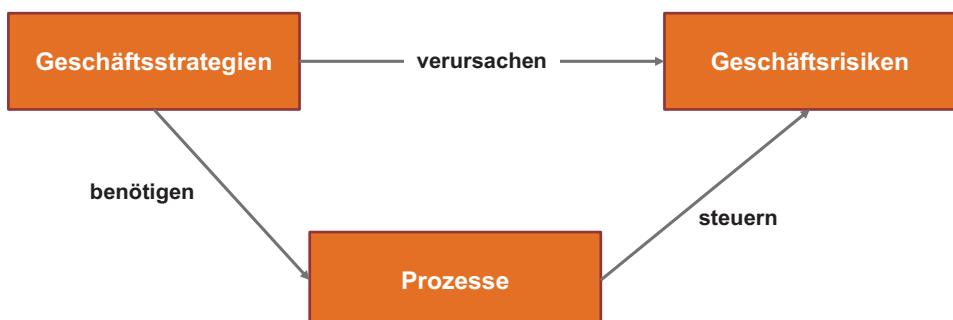


Abb. 1.2 Strategie und Risiko. (Quelle: eigene Darstellung in Anlehnung an Rohlfs 2018, S. 47)

Grundsätzlich können die **notwendigen Prozesse** unterteilt werden in

- Geschäftsprozesse für die Wertschöpfung,
- Informations- und Entscheidungsprozesse für die Unternehmenssteuerung,
- Kontrollprozesse als Risikomanagementprozesse.

Um im Unternehmen eine wert- und risikoorientierte Steuerung umsetzen zu können, braucht man also eine Geschäftsorganisation, die **Kontrollinstanzen bzw. Koordinationsfunktionen** vorsieht. Sämtliche Kontrollaspekte können dabei als Absicherung von Risiken verstanden werden. Entsprechend können finanzielle, technische und organisatorische Risiken abgesichert werden. Mit dem **Risikomanagement** als strukturiertem Umgang mit Chancen und Risiken im Unternehmen (DRS 20.11) versucht man eben diese Risiken zu steuern.

Als **finanzielles Risikomanagement** kann die Absicherung der Bilanz und die Steuerung der Risikotragfähigkeit verstanden werden. Hierzu gehören Instrumente wie Einkauf von Versicherungsschutz, Hedging, alternativer Risikotransfer, Steuerung der Durationslücke, allgemeine Risikostreuung, Liquiditätsmanagement.

Mithilfe des **technischen Risikomanagements** sollen die betriebliche Infrastruktur und die Arbeitsprozesse abgesichert werden. Im Fokus stehen Materialnutzung, Anlagensicherheit, Produktsicherheit & Produkthaftung, Arbeitnehmerschutz & Umweltschutz, Aufrechterhaltung der Geschäftstätigkeit einschließlich dem Business Continuity Management.

Das **organisatorische Risikomanagement** dient der Absicherung der gesamten Geschäftsorganisation im Normalbetrieb und in Krisensituationen. Hierunter fallen sämtliche Maßnahmen im Rahmen der Organisationsstruktur, die sich auf die Ausgestaltung bzw. Sicherung von Aufbau- und Ablauforganisation beziehen. Ebenso verlangt die Steuerung und Kontrolle der Geschäftsorganisation ein funktionierendes Informationssystem.

All diese Schwerpunkte im Risikomanagement bilden das **Risikomanagementsystem** als „Gesamtheit der Regelungen, die einen strukturierten Umgang mit Chancen und Risiken im Unternehmen sicherstellt“ (IDW PS 981, Tz. 17).

Ein solches Risikomanagementsystem muss durch eine unternehmensweite, ganzheitliche und antizipative Betrachtung sämtlicher Risiken in einem bereichsübergreifenden Prozess systematisch und effektiv steuern (vgl. Diederichs 2012, S. 12 f.). Somit werden Risiken nicht mehr isoliert betrachtet, sondern im Unternehmenskontext global analysiert. Der mit dieser Zielsetzung ausgerichtete Ansatz wird auch als **Enterprise Risk Management** bezeichnet (vgl. Rohlfs 2018, S. 1). Das Enterprise Risk Management unterstellt für das Risikomanagement, dass es

- ein Prozess ist, der sich ununterbrochen und über die gesamte Organisation erstreckt;
- durch Menschen auf jeder Ebene einer Organisation ausgeführt wird;
- bereits bei der Strategiefestlegung angewendet wird;
- unternehmensübergreifend angewendet wird (auf jeder Ebene und in jeder Einheit) und das organisationsweite Risikoportfolio betrachtet;

- so gestaltet ist, dass mögliche das Unternehmen beeinflussende Ereignisse erkannt und Risiken auf Grundlage der Risikoneigung gesteuert werden können;
- geeignet ist, den Führungskräften sowie den Überwachungs- und Leitungsorganen einer Organisation hinreichend Sicherheit zu gewährleisten;
- ausgerichtet ist auf das Erreichen von (zusammenhängenden) Zielen (vgl. COSO 2004, S. 2).

Der gewählte Risikomanagementansatz ist natürlich auch im Rahmen der Mehrwert-Betrachtung zu analysieren. So gibt es sicherlich auch Steuerungsmaßnahmen für eingegangene Risiken, die unter Effizienz- und Effektivitätsgesichtspunkten nicht sinnvoll sind. Somit hat auf den **Unternehmenswert** neben der Geschäftsstrategie auch immer der Umgang mit Risiken im Rahmen des Risikomanagementsystems einen wesentlichen Einfluss. Dieser Einfluss kann über ein **Total Cost of Risk-Modell** (TCOR) als gemeinsame Betrachtung von Risikofinanzierung und Risikokontrolle schematisch dargestellt werden (vgl. Abb. 1.3).

Der Total Cost of Risk erfasst alle relevanten Kosten aus dem Management der Risiken und stellt sie den möglichen Verlusten aus der Realisierung der Risiken gegenüber. Somit sind alle ergriffenen Kontroll- und Absicherungsmaßnahmen aus ökonomischer Sicht zu beurteilen, inwieweit diese sich in einer Gesamtbetrachtung positiv auf den Unternehmenswert auswirken.

Zur systematischen Beurteilung wird der Total Cost of Risk in **verschiedene Bestandteile** untergliedert:

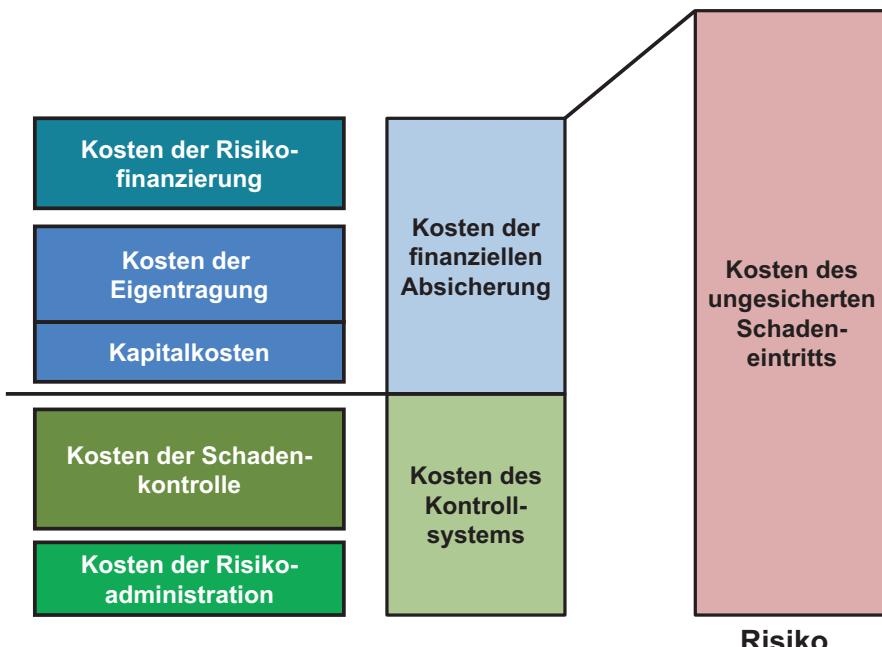


Abb. 1.3 TCOR-Ansatz. (Quelle: eigene Darstellung)

- **Kosten der Risikofinanzierung:** Können Risiken extern abgesichert werden (absicherbare Risiken), sind hier Versicherungsprämien oder Kosten für Kapitalmarktinstrumente zu erfassen.
- **Kosten der Eigentragung:** Hierunter fallen Schadenkosten durch bewusst oder unbewusst nicht versicherte Schäden, nichtversicherbare Schäden und vereinbarte Selbstbeteiligungen. Auch die Kosten für den Einsatz einer firmeneigenen Versicherung (Captive) können hierunter fallen. Die Schadenkosten können in der Bewertung dabei auch mit einer Risikomarge für die mögliche Volatilität der Schadenhöhe versehen werden.
- **Kapitalkosten:** Ansatz von kalkulatorischen Kosten für gebundenes Eigenkapital, das zur Risikofinanzierung benötigt wird.
- **Kosten der Schadenkontrolle:** sämtliche externen und internen Kosten der Kontrollprozesse (Kontrolle des Risikos). Hierzu zählen zum Beispiel Maßnahmen für den Brandschutz, das Qualitätsmanagement oder auch Kontrollen im Rahmen der Geschäftsorganisation.
- **Kosten der Risikoadministration:** Kosten für die interne und externe Administration rund um das Risikomanagement oder auch das Versicherungsmanagement. Hierzu gehören zum Beispiel die Kosten für eine eigene Risikomanagement- und Versicherungsabteilung (ggf. einen firmenverbundenen Versicherungsvermittler) oder auch für den Einsatz eines externen Versicherungsmaklers oder sonstiger eingekaufter Expertise.

Je nach Betrachtungsgegenstand ist der Total Cost of Risk (TCOR) eher ein akademisches Gedankenspiel (zum Beispiel zur Bewertung der Internen Revision als Maßnahme im organisatorischen Risikomanagement). Er kann aber auch konkret in unternehmerische Entscheidungen einfließen, zum Beispiel bei der Auswahl von Versicherungslösungen über den Ansatz der sogenannten „Total Cost of Insurable Risk“ (TCOIR). Mit dem TCOIR werden nur die Kosten gemessen, die dem Unternehmen im Zusammenhang mit dem Einkauf von Versicherungen, dem Einsatz interner und externer Versicherungsberatung (eigene Versicherungsexperten, externe Versicherungsmakler und sonstige) und dem Eigenbehalt bestimmter versicherungsfähiger Risiken (zum Beispiel über Selbstbehalte oder den Einsatz einer Captive-Versicherung) entstehen.

1.2 Risikomanagementprozess

Das Risikomanagementsystem als Unternehmensfunktion im Sinne eines **Enterprise Risk Management** kann einerseits als Absicherungssystem und andererseits als Informationssystem verstanden werden. Das System ist zur Unternehmenssteuerung als fortlaufender Prozess zu gestalten.

Zum klassischen Aufbau eines **Risikomanagementprozesses** gehören die Prozessschritte der Risikoanalyse, der Risikosteuerung sowie der Risikokontrolle und Berichterstattung. Die Risikoanalyse beinhaltet die Identifizierung und Bewertung der Risiken sowie ggf. deren Aggregation.

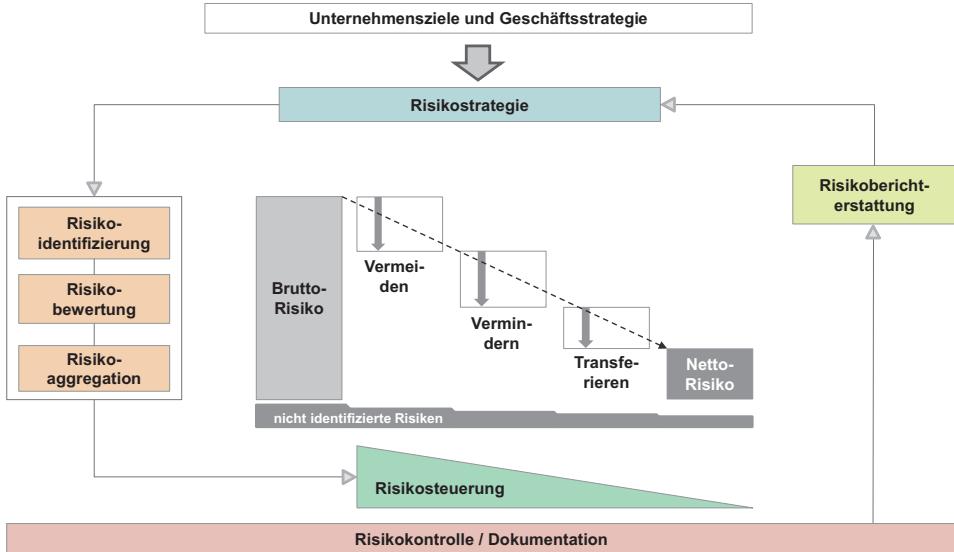


Abb. 1.4 Risikomanagementprozess. (Quelle: eigene Darstellung)

Die Vorgabe der Unternehmensziele und die Aspekte der Risikostrategie und Risikotoleranz (Unternehmensplanung) sind dem eigentlichen Risikomanagementprozess vorgelagert (vgl. Abb. 1.4).

1.2.1 Risikostrategie

Die Risikostrategie schildert insbesondere die Auswirkungen der Geschäftsstrategie auf die **Risikosituation** des Unternehmens und beschreibt den Umgang mit den vorhandenen Risiken und die Fähigkeit des Unternehmens, neu entstehende Risiken zu tragen. Durch die festgelegten Ziele und Entscheidungen, die in der Geschäftsstrategie beschrieben werden, ergeben sich Risiken aus den verschiedenen unternehmensinternen und externen Umweltfaktoren. Ähnlich zu der Beurteilung von miteinander verbundenen Zielen sind unter Risikogesichtspunkten dabei auch Risikozusammenhänge festzustellen (vgl. Rohlfs 2018, S. 49 f.).

In der Risikostrategie werden neben der grundsätzlichen Risikoausrichtung Leitlinien festgelegt, die den Risikomanagementprozess gestalten.

Der **Inhalt der Risikostrategie** muss sich beschäftigen mit

- Art des Risikos,
- Herkunft des Risikos,
- Zeithorizont der Risikobetrachtung,
- Risikotoleranz und
- Risikotragfähigkeit.

Die konkret angestrebte Höhe von Risiko und Risikotragfähigkeit wird über die **Risikobereitschaft** definiert (Risikoappetit und Risikotoleranz).

Beim **Risikoappetit** stellt man sich die Frage, was das Unternehmen sich insgesamt an Risiken erlauben will. Er beschreibt somit die „Haltung“ der Entscheidungsträger gegenüber den wesentlichen Risikokategorien und Risikoarten (vgl. BaFin, Rn. 2.77). Der Risikoappetit gibt an, wie viel des ökonomischen Eigenkapitals zur Abdeckung aller wesentlichen Risiken verwendet werden soll. Er steht für die individuelle Risikobereitschaft der Entscheidungsträger und orientiert sich an den strategischen Zielen des Unternehmens. Der Risikoappetit spiegelt sich in der Risikostrategie wider (vgl. Ellenbürger et al. 2009, S. 166).

Im Hinblick auf die **Risikotoleranz** stellt man sich dagegen die Frage, was das Unternehmen sich erlauben kann bzw. darf. Es kann sich um Beschränkungen handeln, die sich das Unternehmen bei der Übernahme von Risiken selbst auferlegt – der Risikoappetit („erlauben kann“) – oder solche, die die Risikoübernahmekapazität durch externe Vorgaben tatsächlich beschränken („erlauben darf“). Hier kann es sich zum Beispiel um Beschränkungen handeln, um ein marktakzeptables Mindest-Rating zu erhalten oder um ggf.aufsichtsrechtliche Anforderungen zu erfüllen (vgl. BaFin, Rn. 2.77).

1.2.2 Risikoidentifizierung

Risiken ergeben sich aus der Geschäftsstrategie und allen daraus abgeleiteten operativen Tätigkeiten. Um den Umgang mit den Risiken vorgeben zu können, müssen diese zunächst **identifiziert** werden. Dies beinhaltet die möglichst vollständige Erfassung aller Risikobereiche, Risikoursachen und Risikoobjekte.

Riskoidentifizierung beschreibt die Suche und Bestimmung aller Einzelrisiken sowie das Bilden von Risikogruppen bzw. -kategorien. Sie liefert damit Informationen, welche unerlässlich sind, um relevante Risiken systematisieren, analysieren und bewerten zu können. Indem **gleichartige Risiken** zusammengefasst werden, erhalten Unternehmen einen besseren Überblick hinsichtlich der Risiken und auch den damit verbundenen Chancen. Eine **Risikokategorisierung** vereinfacht den gesamten Prozess der Risikoanalyse, insbesondere der Bewertung eines Risikokapitalbedarfs sowie der Erfassung von Diversifikationseffekten. Auch bietet sie den Unternehmen die Möglichkeit, verschiedene Risikoarten mit entsprechend zugeschnittenen Maßnahmen und Instrumentarien zu steuern (vgl. Sartor und Bourauel 2013, S. 10 ff.).

Die Methoden zur Risikoidentifizierung sind vielfältig und können in zwei Bereiche unterteilt werden: Managementmethoden und unterstützende Methoden zur Informationssammlung und -generierung. Unter **Managementmethoden** werden Analyseansätze verstanden, die im Unternehmen zur Bildung der Geschäftsstrategie verwendet werden und daher auch zur Aufdeckung von Risiken verwendet werden. Hierzu zählen beispielsweise Wertschöpfungsketten, SWOT-Analysen, Benchmarks, die Balanced Scorecard etc. Um Informationen zu sammeln oder zu generieren, die bei Anwendung der Managementme-

thoden weiter verarbeitet oder strukturiert werden können, eignen sich dann verschiedene **Kollektions- und Suchmethoden** wie Checklisten, Dokumentenanalysen, Fehlerbaumanalysen, Brainstorming oder Szenario-Techniken.

Das Übersehen von Risiken oder deren zu späte Identifizierung kann zu unternehmerischen Gefahren (bis hin zur Existenzgefährdung) führen. Eine **spätere Fehlerkorrektur** erweist sich häufig als schwierig. Oftmals ist sie mit einem hohen Kostenaufwand verbunden. In der Unternehmenspraxis besteht unter Umständen aber auch die Gefahr, dass ein späteres Eingreifen nicht mehr möglich ist. Da Unternehmen in der heutigen Zeit einem ständigen Wandel und neuen Rahmenbedingungen ausgesetzt sind, ist eine **kontinuierliche und systematische** Risikoidentifizierung und -beobachtung unabdingbar (vgl. Diederichs 2012, S. 50 f.).

Das Ergebnis der Risikoidentifizierung ist eine **strukturierte Darstellung** von allen bestehenden und potenziellen Risiken inklusive ihrer Auswirkungen in einem **Risikokatalog** (Risikoinventar). Ziel der Risikoidentifizierung ist eine möglichst konsistente und überschneidungsfreie Bestandsaufnahme aller Risiken. Durch den Risikoidentifizierungsprozess wird das **Gesamtrisikoprofil** eines Unternehmens bestimmt.

1.2.3 Risikobewertung

Die Risikobewertung verfolgt das Ziel, das von den identifizierten Risiken ausgehende **Gefahrenpotenzial** transparent zu machen und deren Wirkung offen zu legen (vgl. Altenähr et al. 2009, S. 63). Dies geschieht durch die Analyse, welche Bedrohungen von den Risiken ausgehen (unwesentliche, wesentliche oder bestandsgefährdende Risiken). Basis dieser Analyse ist somit die Festlegung von Wesentlichkeitsgrenzen, wobei es Risiken gibt, die quantitativ und andere, die lediglich qualitativ beurteilt werden können.

Die Risikobewertung dient dabei einerseits als Grundlage für die Festlegung der Maßnahmen im Rahmen der Risikosteuerung. Andererseits dient sie zur Bestimmung des einzelnen Risikokapitalbedarfs als Basis für die daran anschließende Aggregation zur Ermittlung eines Gesamtrisikokapitalbedarfs.

Im **ersten Schritt** der Bewertung können Risiken durch folgende Methoden eingeschätzt werden („Allgemeine Bewertungs-/Beurteilungsmethoden“):

- Relevanz einschätzungen,
- Scoring-Modelle,
- ABC/XYZ-Analysen oder
- Ratings (Qualitätsstufen).

Durch diese Methoden können die unterschiedlichen Aspekte eines Risikos verdichtet und die Komplexität der realen Gegebenheiten reduziert werden. Dabei besteht auch die Möglichkeit, Risiken in eine Reihenfolge („Ranking“) zu bringen und entsprechend zu analysieren. Des Weiteren können wesentliche von unwesentlichen Risiken getrennt wer-

den, um einen unwirtschaftlichen Mehraufwand im weiteren Bewertungsverfahren zu verhindern.

Infolgedessen werden im **zweiten Schritt** meist nur Risiken intensiver untersucht und präziser bewertet, die nach erster Einschätzung relevant für das Unternehmen sind. Dies geschieht durch eine Quantifizierung, die mithilfe statistischer Methoden und unter Zugrundelegung eindeutig definierter Größen (Schadenausmaß, Eintrittswahrscheinlichkeit, Streuung) die Risiken misst und die Auswirkungen im Zusammenspiel mit anderen Risiken beurteilt.

Dies kann zum Beispiel durch folgende Methoden erreicht werden („Methoden zur Bewertung des Risikoausmaßes“):

- Ratings (Ausfallwahrscheinlichkeiten),
- Quantitative Risikomatrix,
- Wahrscheinlichkeitsverteilungen,
- Stresstests und Szenariorechnungen.

Wegen der Problematik der möglichen Fehleranfälligkeit komplexer Bewertungsmethoden sind an die Bewertung bestimmte **Qualitätsanforderungen** zu stellen. Grundsätzlich sind anerkannte Risikobewertungsmethoden zu verwenden. Um eine Willkürlichkeit zu vermeiden, ist ein unternehmensweites einheitliches Sicherheitsniveau zu unterstellen. Die zu schätzenden Parameter sollten so gewählt und bestimmt werden, dass eine Vergleichbarkeit und Transparenz gegeben ist. Dort, wo es die Bewertung zulässt, sollten im Idealfall vorhandene aktuelle Marktdaten zum Einsatz kommen.

1.2.4 Risikoaggregation

Ziel der Aggregation im Rahmen der Analyse ist es, den gesamten **Risikokapitalbedarf** eines Unternehmens zu ermitteln, welcher sich auf die Entwicklung von Eigenkapital und Gewinn auswirken kann. Hierfür bedarf es einer allgemein gültigen Definition des Gesamtrisikos auf Basis aller Einzelrisiken. Dabei ist die Aggregation nicht zu verwechseln mit der Summe der Einzelrisiken. Die aggregierten Einzelrisiken sind (sofern keine vollständig positive Korrelation vorliegt) grundsätzlich kleiner als die Summe aller Einzelrisiken. Grund hierfür ist die **Diversifikation**, bei der Risikoausgleichseffekte zwischen den Einzelrisiken berücksichtigt werden.

Die Frage, die sich an die Bestimmung des gesamten Risikokapitalbedarfs anschließt, ist die, inwiefern das Gesamtrisiko auch getragen werden kann: Weist das Unternehmen ausreichend hohes ökonomisches Eigenkapital aus? Diese Frage nach der Überdeckung wird durch das Maß der **Risikotragfähigkeit** veranschaulicht. Sie beschreibt die Fähigkeit, Verluste aus Risiken zu absorbieren, ohne dass daraus eine direkte Gefahr für die Existenz des Unternehmens entsteht:

$$\text{Risikotragfähigkeit} = \frac{\text{ökonomisches Eigenkapital}}{\text{Gesamtrisikokapitalbedarf}} \geq 100\%$$

Je nach Rechnungs- und Bilanzierungsgrundlagen kann die Risikotragfähigkeit zu ökonomischen, ratingbezogenen oder aufsichtsrechtlichen Zwecken ermittelt werden.

1.2.5 Risikosteuerung

Im Rahmen der Risikosteuerung ist sicherzustellen, dass der **Risikoumfang** nicht größer als die angestrebte **Risikotragfähigkeit** ist. Zudem sollte die derzeitige Risikosituation mit den damit verbundenen Chancen in Relation gesetzt werden. Risiken sollten nur eingegangen werden, sofern ihnen ein angemessenes Ertragspotenzial gegenüber steht. Entspricht das **Chancen-Risiko-Verhältnis** nicht den Zielvorstellungen des Unternehmens, wird mittels der Risikosteuerung versucht, die Herstellung der geplanten Soll-Risikosituation zu erreichen (vgl. Vanini 2012, S. 224). Dabei wird das ursprüngliche Bruttorisiko auf ein angemessenes Maß reduziert. Die Risikosteuerung umfasst

- Risikovermeidung,
- Risikoverminderung,
- Risikotransfer.

Das nach den Steuerungsmaßnahmen **verbleibende Restrisiko** (Netto-Risiko) wird dann vom Unternehmen selbst getragen. Auf der einen Seite will man gewisse Ertragspotenziale nutzen und somit Risiken bewusst eingehen, auf der anderen Seite ist die **Selbsttragung** aufgrund von mangelnden adäquaten Steuerungsmaßnahmen zwangsläufig notwendig.

Bei der **Risikovermeidung** wird auf das Eingehen von bestimmten Risiken (prospektiv) gänzlich verzichtet. Dies kann aus Gründen des Risikomanagements sinnvoll sein, wenn die Risiken durch ein unverhältnismäßig hohes Risikopotenzial gekennzeichnet sind. Mit der Risikovermeidung geht aber auch einher, dass auf entsprechende mögliche Chancen (Geschäftsstrategien) verzichtet wird.

Im Rahmen der **Risikoverminderung** wird durch die Beeinflussung der Risikostruktur der gesamte Risikogehalt reduziert, aber nicht vollständig eliminiert. Hier steht den Unternehmen eine Vielzahl von Möglichkeiten zur Verfügung, mithilfe geeigneter Maßnahmen auf die Eintrittswahrscheinlichkeit und/oder das Schadenausmaß eines Risikos einzuwirken. Die Risikoverminderung führt dazu, dass auch weiterhin Ertragspotenziale genutzt werden können, da das eingegangene Risiko und die damit verbundene Chance nicht vollständig ausgeschlossen wird.

Bei der Steuerung können **ursachen- und wirkungsbezogene Maßnahmen** unterschieden werden. Ursachenbezogene Strategien zielen darauf ab, die Eintrittswahrschein-

lichkeit des Risikos zu vermeiden oder zu vermindern. Wirkungsbezogene Maßnahmen hingegen sollen die Auswirkungen bei Realisation des Risikos verringern (vgl. Altenähr et al. 2009, S. 117).

Außerdem können Risiken zur Reduzierung der eigenen Risikoexponierung an einen Dritten **transferiert** werden. Das ursprüngliche Risiko bleibt bestehen, es wird jedoch nicht mehr allein getragen. Eine klassische Form des Risikotransfers ist die Versicherung. Vorstellbar ist aber auch der Transfer von Risiken auf den Kapitalmarkt, auf den Kunden oder auf Lieferanten. Aber auch Ausgliederungen oder die Gründung von Gesellschaften können je nach Gestaltung als Transfer gesehen werden.

Die Abbildung zum Risikomanagementprozess veranschaulicht schematisch, wie das ursprüngliche **Brutto-Risiko** grundsätzlich durch geeignete Steuerungsmaßnahmen auf das beim Unternehmen verbleibende **Netto-Risiko** reduziert werden kann. Neben den identifizierten Risiken besteht trotz umfassender Risikoanalysen die Gefahr, dass Risikopotenzielle nicht erkannt werden. Diese nicht identifizierten Risiken können natürlich nicht bewusst gesteuert werden. Sie werden jedoch unbewusst auch durch die Etablierung allgemeiner Steuerungsmaßnahmen vermindert.

1.2.6 Risikokontrolle und Berichterstattung

Die Risikokontrolle (auch Risikocontrolling) beschreibt ein zusammenfassendes und zugleich steuerndes Element innerhalb des gesamten Risikomanagementprozesses. Sie ist zur Beurteilung von Effizienz und Wirksamkeit des Risikomanagements sowie zur Feststellung möglicher Verbesserungspotenziale erforderlich. Kontrolle verlangt auch immer eine Dokumentation bzw. eine Berichterstattung. Nur eine angemessene Berichterstattung ermöglicht es den verschiedenen Parteien, die in den Risikomanagementprozess eingebunden sind, ihrer Überwachungs- oder Entscheidungsfunktion auf Basis der erhaltenen Informationen nachzukommen.

Die **Risikokontrolle** durch das Risikomanagement beinhaltet im Wesentlichen folgende Aspekte:

- Überprüfung der Angemessenheit der eingerichteten Maßnahmen zum Aufbau und Ablauf des Risikomanagementprozesses (einschließlich der Weiterentwicklung);
- Sicherstellung der vollständigen Erfassung aller wesentlichen Risiken und deren angemessene Beurteilung/Bewertung;
- Kontinuierliche Anwendung der risikorelevanten Maßnahmen bzw. deren Anpassung;
- Einhaltung der integrierten Kontrollen;
- Kommunikation.

Die Prozesse und die Ergebnisse der Risikoanalyse und Risikosteuerung sind laufend zu kontrollieren, damit sichergestellt ist, dass eingegangene Risiken in einem tolerierbaren Ausmaß bleiben. Aus dieser Anforderung heraus ist ein unternehmensweites **Kontroll-**

system zu implementieren, in dem alle operativen Bereiche und das Risikomanagement eingebunden sind. Die Risikokontrolle verlangt dabei natürlich auch eine systematische Dokumentation, um später eine Überprüfung vornehmen zu können.

In der **Risikoberichterstattung** soll über das Risikoprofil des Unternehmens berichtet werden. Sie dient somit der permanenten Überwachung und stellt sicher, dass identifizierte und bewertete Risiken den (internen und externen) Entscheidungsträgern mitgeteilt werden. Bei der Kommunikation kann eine interne und eine externe Berichterstattung unterschieden werden.

Die Unternehmen müssen über eine angemessene und aussagefähige **interne Risikoberichterstattung** verfügen. Es ist Aufgabe des Risikomanagements, die Risikoberichterstattung in Abstimmung mit den verschiedenen Unternehmensbereichen aufzustellen und diese der Geschäftsführung, dem Aufsichtsrat, den entsprechenden Managementebenen, anderen Unternehmensfunktionen und den Mitarbeitern zur Verfügung zu stellen. Dadurch soll sichergestellt werden, dass die Informationsadressaten alle wichtigen Informationen zur Risikosituation erhalten. Die Kommunikation kann **regelmäßig** (zum Beispiel wöchentlich, monatlich, jährlich) oder **ad hoc** erfolgen. Letzteres führt zum Beispiel zu einer sofortigen Meldung bei der Überschreitung eines Schwellenwertes bei einer Risikokennzahl oder dem Eintreten eines außergewöhnlichen Ereignisses.

Für die **externe Berichterstattung** bildet das Handelsgesetzbuch die gesetzliche Grundlage. Gemäß § 264 Abs. 1 HGB ist bei Kapitalgesellschaften der Jahresabschluss, bestehend aus der Bilanz, der Gewinn- und Verlustrechnung und dem Anhang, um einen **Lagebericht** zu erweitern. Aus Sicht der Risikoberichterstattung ist insbesondere der Lagebericht gemäß der **§§ 289 bis 289f HGB** von Bedeutung. Konkretisiert wird die Risikoberichterstattung für den Lagebericht durch den **DRS 20**, der jedoch für Konzernlageberichte gilt. Die Anwendung des DRS 20 auf den Einzelabschluss ist somit nicht zwingend, sie wird aber empfohlen (vgl. DRS 20, Tz. 2). Aus diesem Grund kann er als Rahmenwerk für eine angemessene öffentliche Berichterstattung angesehen werden.

Die externe Berichterstattung kann in Abhängigkeit von speziellen Zielsetzungen (wie Verkaufsprospekte) oder Branchen (wie die aufsichtsrechtliche Berichterstattung bei Versicherungsunternehmen oder Banken) zusätzlich variieren.

Literatur

- Altenähr, V., Nguyen, T., & Romeike, F. (2009). *Risikomanagement kompakt*. Karlsruhe: Versicherungswirtschaft.
- Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). (2016). Erläuterungen zu Leitlinien zum Governance-System der EIOPA, Übersetzung durch die BaFin, 20.05.2016. https://www.bafin.de/SharedDocs/Downloads/DE/Aufsichtsrecht/dl_erp_texte_leitlinien_zu_governance_system_de_va.html?nn=7850436. Zugegriffen am 04.03.2020.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2004). COSO II, Unternehmensweites Risikomanagement – Übergreifendes Rahmenwerk, Zusammenfassung, September 2004.

- Deutscher Rechnungslegungs Standard Nr. 20 (DRS 20). (2012). Konzernlagebericht, Deutsche Rechnungslegungs Standards Committee/DRSC (Hrsg.), 2012.
- Diederichs, M. (2012). *Risikomanagement und Risikocontrolling* (3. Aufl.). München: Franz Vahlen GmbH.
- Ellenbürger, F., Ott, P., Frey, C., & Boetius, F. (2009). *Mindestanforderungen an das Risikomanagement (MaRisk) für Versicherungen – Eine einführende Kommentierung*. Schäffer-Poeschel.
- Institut der Wirtschaftsprüfer. (2017). IDW Prüfungsstandards, Grundsätze ordnungsmäßiger Prüfung von Risikomanagementsystemen (IDW PS 981), Düsseldorf.
- Lange, O. (2014). *D&O-Versicherung und Managerhaftung*. München: C.H. Beck.
- Rohlfs, T. (2018). *Risikomanagement im Versicherungsunternehmen* (2. Aufl.). Karlsruhe: Versicherungswirtschaft.
- Rohlfs, T., Savic, B., & Will, D. (2019). *Rechnungslegung und Controlling der Versicherungsunternehmen*. Karlsruhe: Versicherungswirtschaft.
- Sartor, F. J., & Bourauel, C. (2013). *Risikomanagement kompakt – In 7 Schritten zum aggregierten Nettorisiko des Unternehmens*. Oldenbourg Wissenschaftsverlag.
- Vanini, U. (2012). *Risikomanagement: Grundlagen, Instrumente, Risikopraxis*. Stuttgart: Schäffer-Poeschel.

Prof. Dr. Torsten Rohlfs lehrt am Institut für Versicherungswesen der Technischen Hochschule Köln. Seine Fachgebiete sind insbesondere das Rechnungswesen und Risikomanagement von Versicherungsunternehmen. Er ist Wirtschaftsprüfer und war vor seiner Tätigkeit an der TH Köln Senior Manager bei der KPMG AG Wirtschaftsprüfungsgesellschaft im Bereich Prüfung und Beratung von Versicherungsunternehmen. Prof. Dr. Torsten Rohlfs ist Mitglied im Ratingkomitee der ASSEKURATA Assekuranz Rating-Agentur GmbH und im wissenschaftlichen Beirat des Gesamtverbands der versicherungsnehmenden Wirtschaft e.V. (GVNW). Darüber hinaus ist er Mitglied der Prüfungskommission für Wirtschaftsprüfer.

Dr. Alexander Mahnke begann seine berufliche Laufbahn im Jahr 1999 bei Siemens, wo er zuletzt bei SFS für die Koordination der weltweiten Konzern-Haftpflichtversicherungsprogramme zuständig war. Von 2004 bis 2010 war er bei AON Jauch & Hübener unter anderem als Leiter des Geschäftsfelds Financial Services Group tätig. 2010 übernahm er bei Marsh die Leitung der beiden Geschäftsgebiete Financial & Professional Services (FINPRO) und Credit & Political Risks und wurde Anfang 2011 in die erweiterte Geschäftsleitung der Marsh GmbH berufen.

Im April 2011 übernahm er die Leitung Versicherungen bei Siemens in München und ist in dieser Funktion für alle versicherungsfähigen Risiken des Konzerns weltweit zuständig.

Dr. Alexander Mahnke ist Vorsitzender des Vorstandes des Gesamtverbandes der versicherungsnahmenden Wirtschaft e. V. (GVNW).

Er hat Rechtswissenschaften in Bayreuth, München und Montpellier studiert und an der Universität Bochum promoviert.

Teil II

Risikomanagementprozess



Risikoidentifizierung und -klassifizierung

2

Wolfgang Knauf und Jessica Bender

Zusammenfassung

In diesem Kapitel wird der erste Schritt des Risikomanagementprozesses erläutert. Bei der Risikoidentifizierung geht es darum, unter Beachtung der Vollständigkeit, Wirtschaftlichkeit, Zukunftsbezogenheit, Aktualität und Konsistenz, diejenigen Entwicklungen oder Ereignisse zu bestimmen, die zu einer für ein Unternehmen negativen Prognose- oder Zielabweichung führen können. Dabei kann ein Unternehmen aus verschiedenen Perspektiven an die Identifizierung herangehen und aus einer Vielzahl an Risikoidentifizierungsmethoden wählen. Wurden alle relevanten Risiken identifiziert, findet dann die Risikoklassifizierung statt. Hierbei werden die zuvor identifizierten Risiken den unternehmensindividuell gebildeten Klassen zugeordnet. Innerhalb der Risikoklassen hat ein Unternehmen die Möglichkeit noch weitere Systematisierungen der Risiken vorzunehmen. Sind Risikoidentifizierung und -klassifizierung abgeschlossen, werden die Ergebnisse strukturiert dargestellt.

2.1 Aufgabe der Risikoidentifizierung

Um zu verdeutlichen, worum es bei der Risikoidentifizierung geht, werden zunächst einmal die beiden Begriffe „Risiko“ und „Identifizierung“ definiert.

W. Knauf (✉)
Henkel AG & Co. KGaA, Düsseldorf, Deutschland
E-Mail: wolfgang.knauf@henkel.com

J. Bender
TH Köln, Institut für Versicherungswesen, Köln, Deutschland
E-Mail: bender.jessica@t-online.de

Je nach Kontext, wird der Begriff „Risiko“ anders verwendet. Allgemein kann jedoch unter einem Risiko eine Abweichung von einem erwarteten Ergebnis verstanden werden. In diesem Buch wird die Risikodefinition des DRS 20 zugrunde gelegt, welche Ergebnisabweichung in positive oder negative Abweichungen differenziert. „Mögliche künftige Entwicklungen oder Ereignisse, die zu einer für das Unternehmen negativen Prognose- oder Zielabweichung führen können“ (DRS 20, Tz. 11), werden im Folgenden als Risiko bezeichnet. Während „mögliche künftige Entwicklungen oder Ereignisse, die zu einer für das Unternehmen positiven Prognose- oder Zielabweichung führen können“ (DRS 20, Tz. 11) als Chancen für das Unternehmen verstanden werden.

Der Begriff „Identifizierung“ wird im Alltag oft im Zusammenhang mit der Identifizierung von Menschen, zum Beispiel anhand eines Personalausweises benutzt. Doch genauso wie Menschen anhand von gewissen Merkmalen identifiziert werden können, können auch Risiken identifiziert werden. Dazu wird die Definition von einem Risiko zur Hilfe genommen, um nach allen Entwicklungen oder Ereignissen zu suchen, die ein Risiko für das Unternehmen darstellen könnten.

In einem Unternehmen gibt es zahlreiche Risiken, welche die Ziele und damit die ganze Unternehmung an sich gefährden können. Die Risiken ergeben sich nicht nur aus der verfolgten Geschäftsstrategie, sondern auch aus dem operativen Geschäft. Damit die Risiken jedoch zu keinen existenzbedrohenden Gefahren für das Unternehmen werden, bedarf es einen strukturierten Umgang mit diesen Risiken. Den Rahmen dafür bildet der Risikomanagementprozess. Beginnend mit der Risikoidentifikation werden die Risiken im Laufe des Prozesses noch bewertet, aggregiert und durch Risikosteuerungsmaßnahmen gemindert oder sogar ganz vermieden. Die Risikoidentifizierung ist deshalb so wichtig, weil ein Unternehmen zunächst einmal wissen muss, welchen Risiken es überhaupt ausgesetzt ist, um überhaupt geeignete Maßnahmen einleiten zu können (vgl. Siemens und Dahms 2014, S. 1).

Ziel der Risikoidentifizierung ist es, alle aktuellen, zukünftigen und potenziellen Einzelrisiken für das Unternehmen aufzudecken und zu erfassen. Denn werden Risiken nicht identifiziert, werden sie im Risikomanagementprozess auch nicht weiter betrachtet (vgl. DIN 2010, S. 10).

2.1.1 Anforderungen an die Risikoidentifizierung

Da die Risikoidentifizierung als Grundlage für alle anderen Schritte im Risikomanagementprozess dient, sollte sie möglichst strukturiert in einem Unternehmen durchgeführt werden. Um dies zu gewährleisten, müssen bestimmte Anforderungen an die Identifizierung gestellt werden. Die geläufigsten Anforderungen sind folgende fünf (vgl. Rohlfs 2018, S. 98):

1. Vollständigkeit,
2. Wirtschaftlichkeit,

3. Zukunftsbezogenheit,
4. Aktualität,
5. Konsistenz.

Bezüglich der **Vollständigkeit** muss darauf geachtet werden, dass die Risikoidentifikation möglichst detailliert und lückenlos erfolgt. Dabei sollen alle aktuellen, zukünftigen sowie potenziellen Risiken aufgedeckt werden. Wird diese Anforderung nicht eingehalten, dann besteht die Gefahr, dass einzelne Risiken nicht erkannt werden. Diese können dann logischerweise nicht im weiteren Verlauf des Prozesses berücksichtigt werden, sodass das Unternehmen keine Möglichkeit hat geeignete Gegenmaßnahmen einzuleiten und im schlimmsten Fall durch diese nicht erkannten Risiken in der Zukunft Verluste erleidet (vgl. Diederichs 2018, S. 93).

Bei der Anforderung an die **Wirtschaftlichkeit** geht es darum, eine Kosten-Nutzen-Betrachtung durchzuführen. Hierbei sollen die Kosten, die ein Risikoidentifizierungsprozess verursacht, in Relation zum Nutzen, also der Menge und der Qualität der erzielbaren Erkenntnisse, gesetzt werden. Dabei kommt es vor allem darauf an, nur die wesentlichen Risiken zu erfassen (vgl. Rohlf 2018, S. 98). Nimmt die Risikoidentifizierung beispielsweise eine erhebliche Zeit in Anspruch und bindet damit wertvolle Mitarbeiterressourcen, gleichzeitig wurden aber bereits alle wesentlichen Risiken aufgedeckt, dann ist es unwirtschaftlich für das Unternehmen den Identifizierungsprozess weiter laufen zu lassen und nur noch Risiken zu erfassen, welche lediglich einen geringen Einfluss auf das Unternehmen haben. Genauso ist es bei der Methodenwahl. Es sollten nach Möglichkeit nur die wirtschaftlich sinnvollsten Methoden für das Unternehmen gewählt werden (vgl. Siemens und Dahms 2014, S. 10).

Auch sollte eine Risikoidentifizierung immer **zukunftsbezogen** erfolgen. Das heißt, dass das Unternehmen vorausschauend denken muss und Veränderungen im Umfeld des Unternehmens mitberücksichtigen sollte. Diese Veränderungen sollten vom Unternehmen sowohl prospektiv als auch antizipativ betrachtet werden. Bei der prospektiven Betrachtung wird versucht aus den Vergangenheitsdaten zu analysieren, welche Risiken in Zukunft entstehen könnten, wobei zum Beispiel erkennbare Trends weiterverfolgt werden können. Bei der antizipativen Betrachtung geht es um die von Vergangenheitsdaten losgelöste Suche nach Risiken, die in Zukunft das Unternehmen gefährden könnten (vgl. Rohlf 2018, S. 98).

Hinsichtlich der **Aktualität** ist gefordert, dass die Risikoidentifizierung kontinuierlich und frühzeitig durchgeführt wird. Durch das sich immer verändernde Umfeld des Unternehmens ist es wichtig, jederzeit die aktuelle Situation abzubilden und regelmäßig neu die Risiken zu identifizieren. Vor allem sollte diese Identifizierung aber früh genug geschehen, um noch rechtzeitig mit präventiven Maßnahmen agieren zu können. Wurde ein Risiko zu spät identifiziert, kann das Unternehmen oft nur noch reagieren, was bedeutet, dass das Risiko bereits eine tatsächliche Gefahr für das Unternehmen darstellt (vgl. Diederichs 2018, S. 93).

Des Weiteren sollte die Anforderung einer **konsistenten** Risikoidentifizierung beachtet werden. Hierbei geht es darum, dass Risiken möglichst eindeutig und überschneidungsfrei identifiziert werden. Diese Anforderung dient als Vorausbereitung für die auf die Risikoidentifizierung folgende Risikoklassifizierung. Wurden die Risiken eindeutig und überschneidungsfrei erfasst, ist eine spätere Klassifizierung einfacher vorzunehmen. Diese sind für den weiteren Verlauf des Risikomanagementprozesses wichtig, da beispielsweise gleichartige Risiken bei der Risikobewertung auch gleichen Bewertungsgrundsätzen unterliegen (vgl. Rohlfs 2018, S. 99).

Wie in den näheren Beschreibungen zu den Anforderungen zu sehen ist, kann ein Unternehmen nicht alle Anforderungen gleichzeitig optimieren. So stehen beispielsweise die Vollständigkeit und die Wirtschaftlichkeit einer Risikoidentifizierung in Konkurrenz zueinander. Ein Unternehmen kann also nur für sich individuell priorisieren, welche Anforderungen an erster Stelle stehen und muss dann bei der Optimierung der Anforderungen Kompromisse eingehen (sogenannter Trade-off; vgl. Diederichs 2018, S. 94).

2.2 Durchführung der Risikoidentifizierung

Unter Beachtung der allgemeinen Anforderungen an die Risikoidentifizierung gibt es verschiedene Ansätze, wie an die Identifizierung von Risiken herangegangen werden kann und auch diverse Methoden, die dabei verwendet werden können.

2.2.1 Ansätze zur Herangehensweise an die Risikoidentifizierung

Wie ein Unternehmen bei der Risikoidentifizierung vorgeht, hängt vor allem von seinen Interessenschwerpunkten ab und aus welcher Perspektive es auf die Risiken blickt. Je nach Perspektive wird die Risikoidentifizierung beispielsweise ausgehend von den Risikoursachen oder auf der Ebene des Unternehmensmanagements durchgeführt. Generell können vier allgemein gültige Ansätze unterschieden werden, wie in Abb. 2.1 dargestellt.

Bei dem **progressiven Ansatz** werden die Risiken des gesamten Unternehmens ausgehend von den Risikoquellen des Unternehmens identifiziert. Zunächst fragt sich das Unternehmen, in welchen Bereichen des Unternehmens Risiken auftreten können, um risiko-



Abb. 2.1 Vier Ansätze zur Herangehensweise an die Risikoidentifizierung. (Quelle: eigene Darstellung in Anlehnung an Rohlfs 2018, S. 99)

behaftete Unternehmensbereiche aufzudecken. Dann werden die Ursachen für diese Risiken bestimmt, indem die Entstehung eines Risikos solange zurückverfolgt wird, bis die Risikoquelle gefunden ist. Im Anschluss wird dann erst geschaut, wie sich die Risikoquellen auf die Unternehmensziele auswirken können. Die Risikoquellen werden hiermit also als der Ursprung des Risikowirkungsprozesses gesehen, der die Unternehmensziele oder -strategie gefährden kann. Dieser Ansatz führt zu einer nahezu vollständigen Erfassung von Risiken, da das gesamte Unternehmen auf alle Risikoquellen hin untersucht wird (vgl. Diederichs 2018, S. 95).

Beim **retrograden Ansatz** hingegen bilden die vorhandenen Unternehmensziele und -strategien die Ausgangsbasis. Hierbei werden direkt die Risiken identifiziert, die unmittelbare Auswirkungen auf diese Ziele und Strategien haben. Dafür müssen zunächst alle definierten Ziele aus den verschiedenen Unternehmensebenen und auch die Ziele des Gesamtunternehmens als Grundlage herangezogen werden. Wurden in einer Unternehmensebene noch keine Ziele formuliert, müssen diese erst einmal hergeleitet werden. Dann wird untersucht, welche Risiken das Unternehmen daran hindern können, diese definierten Ziele zu erreichen. In welchen Unternehmensbereichen diese Risiken verursacht werden, wird erst anschließend betrachtet. Der Vorteil dieses Ansatzes liegt darin, dass Risiken zielgerichteter gesucht und identifiziert werden. Dies ist in der Regel weniger aufwändig als der progressive Ansatz und geht daher oft schneller (vgl. Diederichs 2018, S. 96).

Bei dem **Top-down-Ansatz** beginnt die oberste Ebene des Unternehmensmanagements mit der Risikoidentifizierung, bevor die nachfolgenden Hierarchieebenen den Prozess der Risikoidentifizierung fortsetzen. Dieser Ansatz hat den Vorteil, dass die relevanten Risiken zügig identifiziert werden und der Aufwand relativ gering ist. Allerdings kann es hierbei auch vorkommen, dass die relevanten Risiken, die in den unteren Unternehmensebenen später noch identifiziert werden, nicht mehr zusammengetragen werden und mögliche Abhängigkeiten zwischen verschiedenen Risiken nicht erkannt werden, was ein Nachteil dieses Ansatzes ist (vgl. Sartor und Bourauel 2013, S. 41).

Im Gegensatz dazu wird beim **Bottom-up-Ansatz** auf der niedrigsten Hierarchieebene in den operativen Einheiten des Unternehmens mit der Risikoidentifizierung begonnen. Die Mitarbeiter dort identifizieren die Risiken unmittelbar, mit welchen sie bei ihrer täglichen Arbeit konfrontiert werden können. Danach geht der Risikoidentifizierungsprozess weiter auf die oberen Hierarchieebenen. Der Vorteil dabei ist, dass wenn die Risikoidentifizierung auf der obersten Managementebene endet, dort alle relevanten Risiken an einer zentralen Stelle zusammengetragen wurden. Die Kehrseite dieser vollständigen Erfassung ist jedoch der hohe Aufwand, der dafür betrieben werden muss (vgl. Sartor und Bourauel 2013, S. 41).

Durch die Ausdifferenzierung dieser vier Ansätze soll jedoch nicht der Eindruck entstehen, dass ein Unternehmen sich für einen einzigen davon entscheiden muss. Oft ist es sogar sinnvoll mehrere Ansätze miteinander zu kombinieren. So kann nach einer zunächst einmal retrograden Identifizierung von Risiken der progressive Ansatz genutzt werden, um im Sinne einer vollständigen Erfassung weitere Risiken zu ermitteln. Oder es erfolgt erst eine grobe Identifizierung der relevanten Risiken nach dem Top-down -Ansatz, bevor

diese Identifizierung durch den Bottom-up Ansatz noch weiter konkretisiert wird (vgl. Rohlfs 2018, S. 100 f.).

Um zu zeigen, dass diese Ansätze auch in der Unternehmenspraxis angewendet werden, soll die Henkel AG & Co. KGaA als Praxisbeispiel dienen. In diesem Unternehmen findet einmal jährlich eine Risikoinventur statt, bei der die Unternehmensrisiken identifiziert werden. Die Risikoinventur beginnt sowohl in den lokalen Forschungs- und Entwicklungsstandorten als auch in den lokalen Produktions- und Vertriebsstandorten der verschiedenen Länder, in denen Henkel tätig ist. Bei Betrachtung der Unternehmenshierarchie fällt auf, dass dies die niedrigste Hierarchieebene des Unternehmens ist. Nachdem die Identifizierung auf Länderebene stattgefunden hat, geht der Risikoidentifizierungsprozess weiter bei den Experten der einzelnen Unternehmensbereiche und Zentralfunktionen. Zuletzt werden alle identifizierten Risiken im Bereich Corporate Accounting zusammengetragen. Ein solches Vorgehen bei der Risikoidentifizierung ist ein gutes Beispiel für einen Bottom-up-Ansatz. Neben der jährlichen Risikoinventur ist nicht auszuschließen, dass eine weitere Risikoidentifizierung nach anderen Ansätzen im Unternehmen durchgeführt wird (auch ad hoc) (Henkel AG & Co. KGaA 2018, S. 107 f.).

2.2.2 Methoden zur Risikoidentifizierung

Es gibt diverse Methoden zur Risikoidentifizierung und für ein Unternehmen ist es wichtig, möglichst viele von ihnen zu kennen. Denn wenn ein Unternehmen weiß, welche Methoden es gibt, kann es die vorteilhaften Methoden für den eigenen Risikoidentifizierungsprozess auswählen. Werden Methoden gewählt, die für die jeweilige Zielsetzung unpassend sind, kann dies zur Folge haben, dass die Unternehmensrisiken unzureichend identifiziert werden, was wiederum negative Folgen für die weiteren Schritte im Risiko-Managementprozess hat.

Generell können die Methoden in zwei Gruppen unterteilt werden. In Managementmethoden sowie Methoden zur Informationssammlung und -generierung. Bei den Managementmethoden handelt es sich um Ansätze, die zur Bildung der Geschäfts- und Risikostrategie dienen, mit denen aber auch Risiken aufgedeckt werden können. Bei der zweiten Gruppe werden Informationen zunächst nur generiert und gesammelt, können aber dann auch für die Managementmethoden genutzt werden, wo sie weiterverarbeitet werden (vgl. Rohlfs 2018, S. 103). In diesem Kapitel soll nur eine grobe Übersicht über risikoidentifizierende Methoden gegeben werden, sodass nicht alle existierenden Methoden genannt werden können.

2.2.2.1 Managementmethoden

Die Managementmethoden werden zunächst in Ansätze unterschieden, die sich auf die unternehmensinternen Risiken fokussieren, und andere, die sich auf Risiken fokussieren, die außerhalb des Unternehmens entstehen können. Bei den Methoden mit dem internen Fokus kann entweder der retrograde Ansatz gewählt werden, indem die Unternehmens-

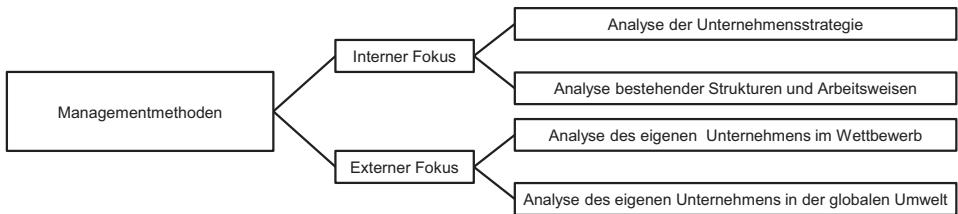


Abb. 2.2 Managementmethoden. (Quelle: eigene Darstellung in Anlehnung an Rohlfs 2018, S. 104)

strategie analysiert wird, oder es wird der progressive Ansatz gewählt, bei welchem die bestehenden Strukturen und Arbeitsweisen betrachtet werden. Bei den Methoden mit dem externen Fokus wird das Unternehmen entweder im Wettbewerb oder in der globalen Umwelt auf Risiken analysiert (vgl. Abb. 2.2; vgl. Rohlfs 2018, S. 103 f.).

Methoden zur Analyse der Unternehmensstrategie

Diese Methoden verfolgen den retrograden Ansatz, sodass die Risikoidentifizierung ausgehend von den Unternehmenszielen durchgeführt wird. Eine beispielhafte Methode für diese Kategorie ist die Balanced Scorecard.

Bei der **Balanced Scorecard** wird zunächst die strategische Unternehmensausrichtung ganzheitlich betrachtet, indem vier unterschiedliche Perspektiven eingenommen werden: Die interne Perspektive, die finanzwirtschaftliche Perspektive, die Kundenperspektive und die Lern- und Entwicklungsperspektive. Diese Perspektiven sollen aus Sicht der Stakeholder (Mitarbeiter, Investoren, Kunden etc.) einen ganzheitlichen Blick auf die Unternehmensausrichtung geben. Je Perspektive werden dann Unterziele formuliert und passende Kenngrößen zur Messung der Zielerreichung ausgewählt. Diese können zum Beispiel der Krankenstand der Mitarbeiter, die Kapitalrentabilität, die Kundentreue oder die Entwicklungsdauer neuer Produkte sein. Anschließend erfolgt ein Soll-Ist-Abgleich dieser Kenngrößen. Die Ergebnisse dieses Abgleiches können frühzeitig auf künftige Negativentwicklungen hinweisen und somit mögliche Risiken bestimmen, welche die Unternehmensziele gefährden können (vgl. Rohlfs 2018, S. 105 f.).

Methoden zur Analyse bestehender Strukturen und Arbeitsweisen

Bei diesen Methoden werden die Risiken ausgehend von den Risikoquellen identifiziert, da sie den progressiven Ansatz verfolgen. Die Prozesskettenanalyse zum Beispiel ist eine solche Methode.

Die **Prozesskettenanalyse** betrachtet die horizontal oder vertikal angeordneten Geschäftsprozesse, in die ein Unternehmen gegliedert werden kann. Diese Prozesse müssen nicht zwingend innerhalb einer Funktion ablaufen, sondern können auch funktionsübergreifend erfolgen. Sind im Unternehmen keine vollständigen oder aktuellen Aufzeichnungen über die Geschäftsprozesse vorhanden, müssen diese Prozesse neu modelliert werden.

Die Geschäftsprozessmodellierung kann dabei in mathematischer, tabellarischer oder grafischer Form durchgeführt werden. Die grafische Darstellung wird dabei sehr häufig genutzt, da bei ihr die Prozessschritte, zum Beispiel durch Zeichnung einer ereignisgesteuerten Prozesskette (EPK), für den Betrachter besonders einfach und selbsterklärend sind. Liegen alle Geschäftsprozesse vor, können nun intuitiv Quellen in den Prozessen lokalisiert werden, von denen Risiken ausgehen können. Mit bereits existierenden Aufzeichnungen über Geschäftsprozesse kann eine Risikoidentifizierung also sehr schnell durchgeführt gehen, andernfalls ist es natürlich ein großer Aufwand, wenn die Geschäftsprozesse erst noch erfasst werden müssen (vgl. Diederichs 2018, S. 105 ff.).

Methoden zur Analyse des eigenen Unternehmens im Wettbewerb

Da es eine ständige Weiterentwicklung der Märkte gibt, sollte auch immer wieder das Wettbewerbsumfeld des Unternehmens analysiert werden, um dort entstehende Risiken zu identifizieren. Eine mögliche Methode, um dies zu tun, ist die Five Forces-Analyse nach Porter.

Porter strukturiert eine Branche in seiner **Five Forces-Analyse** in fünf Wettbewerbskräfte (vgl. Abb. 2.3): Die neuen Wettbewerber, die Käufer, die Lieferanten, die Substitute und die Wettbewerbsintensität. Diese Einteilung in fünf Wettbewerbskräfte kann auf alle Branchen angewendet werden.

Anhand dieser fünf Wettbewerbskräfte wird eine strategische Begutachtung der Brancheaktivitäten durchgeführt, welche die Risiken der eigenen Position des Unternehmens im Marktumfeld aufdecken soll. Dazu wird der aktuelle Stand im Wettbewerbsmarkt betrachtet und mögliche zukünftige Entwicklungen der jeweiligen Wettbewerbskräfte auf Risiken untersucht (vgl. Rosenkranz und Missler-Behr 2005, S. 36). Bei der Wettbewerbskraft „neue Wettbewerber“ können neue Unternehmen, die in den Markt eintreten wollen, denkbare Risiken darstellen, wobei hier auch möglicherweise vorhandene Markteintritts-

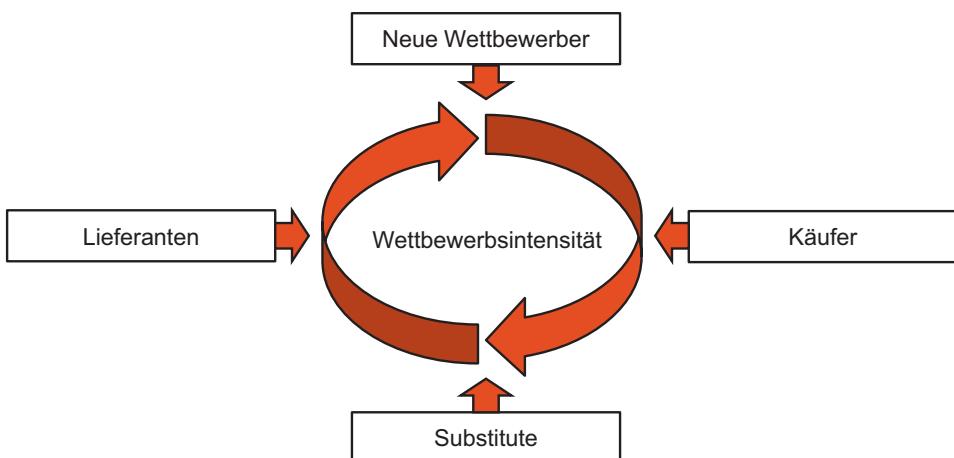


Abb. 2.3 Five Forces Analyse (eigene Darstellung in Anlehnung an Rohlfs 2018, S. 110)

barrieren berücksichtigt werden sollten. Die Marktmacht von Käufern und Lieferanten sollte ein Unternehmen niemals unterschätzen, ebenfalls wie die möglichen Risiken, die sich aus diesen Wettbewerbskräften ergeben könnten. Veränderte Preise der Lieferanten oder veränderte Erwartungen der Kunden sind dabei nur zwei Beispiele. Bei der Wettbewerbskraft „Substitute“ sollte ein Unternehmen nicht nur die Risiken aufdecken, die sich aus neuen Produkten ergeben, welche die eigenen Produkte des Unternehmens ersetzen könnten, sondern auch ganze Geschäftsmodelle berücksichtigen, welche die eigene Unternehmung substituieren könnten. Letztlich sind noch die Risiken vom Unternehmen zu identifizieren, die sich aus der Wettbewerbskraft „Wettbewerbsintensität“ und dem daraus entstehenden Preis- und Qualitätsdruck ergeben (vgl. Rohlfs 2018, S. 110 f.).

Methoden zur Analyse des eigenen Unternehmens in der globalen Umwelt

So, wie sich das Wettbewerbsumfeld des Unternehmens kontinuierlich verändert, verändert sich entsprechend dessen globale Umwelt. Daher ist es wichtig, auch diese regelmäßig auf Risiken hinsichtlich der eigenen Unternehmung zu untersuchen. Dies kann beispielsweise durch die PESTEL-Analyse geschehen.

Mit der **PESTEL-Analyse** soll das Unternehmen einen Überblick über seine allgemeinen Umweltfaktoren erhalten. Dabei bestehen die Buchstaben, aus denen sich der Name der Analyse zusammensetzt, für die sechs Bereiche der Makroumwelt des Unternehmens: Political, Economical, Socio-cultural, Technological, Ecological und Legal. Aus diesen Umweltbereichen werden alle vom Unternehmen als relevant erachteten Faktoren herausgearbeitet. Im politischen Bereich können dies zum Beispiel die Steuerpolitik oder die Stabilität der Regierung sein und im ökonomischen Bereich die Inflation oder Konjunkturzyklen. Im gesellschaftlichen Bereich könnte ein Unternehmen beispielsweise die öffentliche Meinung als bestimmenden Faktor erarbeiten und im technologischen Bereich die neuen Kommunikationsmedien oder eine digitale Wirtschaft. Im ökologischen Bereich wären erneuerbare Energien oder das Achten auf Nachhaltigkeit mögliche bestimmende Faktoren, genauso wie es im rechtlichen Bereich Änderungen im Sozial- oder Arbeitsrecht sein könnten. Hat ein Unternehmen die für sich relevanten Faktoren bestimmt, kann es dann die Risiken identifizieren, welche sich aus diesen Faktoren heraus auf die Unternehmung auswirken könnten (vgl. Rohlfs 2018, S. 113 f.).

2.2.2.2 Methoden zur Informationssammlung und -generierung

Diese Methoden haben die ausschließliche Absicht der Sammlung und Erhebung von Risiken. Oft dienen sie als Vorbereitung für die Managementmethoden, in denen die hier identifizierten Risiken weiter analysiert werden können. Zum reinen Zwecke der Risiko-identifizierung reicht jedoch bereits das Aufdecken der Risiken. Die Methoden lassen sich in Kollektions- und Suchmethoden unterteilen. Während bei den Kollektionsmethoden bestehende offensichtliche Risiken zusammengetragen werden, eignen sich Suchmethoden darüber hinaus noch, um zukünftige Risiken aufzudecken. Die Suchmethoden können dann noch weiter unterteilt werden in analytische Methoden und Kreativitätstechniken (vgl. Abb. 2.4; vgl. Rohlfs 2018, S. 115).

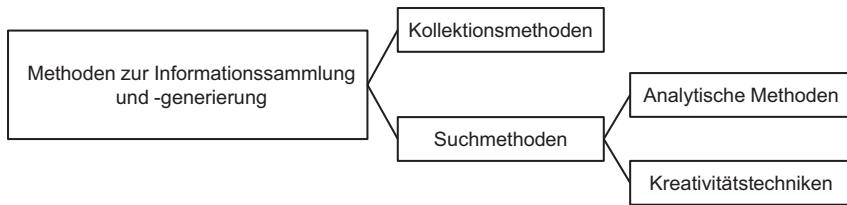


Abb. 2.4 Methoden zur Informationssammlung und -generierung (eigene Darstellung)

Kollektionsmethoden

Methoden zum Zusammentragen bestehender offensichtlicher Risiken gibt es viele. Zwei davon sind Checklisten und Interviews.

Bei **Checklisten** handelt es sich um Listen zur vollständigen Betrachtung der Risiken. Die betrachteten Risiken werden abgehakt („gecheckt“), sodass auffällt, wenn ein Risiko vergessen wurde. Das eigentliche Zusammentragen der Risiken geschieht bei der Erstellung der Checkliste, was auch der aufwändigere Teil der Methode ist. Ist die Checkliste einmal erstellt, kann sie jederzeit wiederverwendet werden und es kann eine Risikoidentifizierung mit relativ geringem Aufwand durchgeführt werden. Für ein Unternehmen, welches bereits viel Erfahrung in der Risikoidentifizierung hat, ist diese Methode also ein gutes Instrument zur zügigen Vollständigkeitsüberprüfung der Risiken. Auch lässt sich eine Checkliste einfach weiterentwickeln, indem einfach weitere Risiken zur Liste hinzugefügt werden. Der Nachteil dieser Methode ist, dass eine Checkliste logischerweise nur die Risiken enthält, die dem Unternehmen aus der Vergangenheit bereits bekannt sind. Die meisten Risiken werden damit wahrscheinlich abgedeckt sein, doch durch stetige Veränderungen innerhalb und außerhalb des Unternehmens entstehen kontinuierlich auch neue Risiken, sodass eine Checkliste niemals vollständig sein kann. Ein Unternehmen sollte bei seiner Risikoidentifizierung also nicht nur auf die Risiken aus einer Checkliste schauen (vgl. Romeike 2018, S. 61 f.).

Interviews können auf verschiedene Arten und mit verschiedenen Personen durchgeführt werden. Experteninterviews eignen sich zum Beispiel gut zur Risikoidentifizierung, da Experten mit ihrem Spezialwissen neue Denkanstöße zu möglichen Risiken liefern und auch selbst relevante Risiken für ihren Fachbereich identifizieren können. Um dadurch eine möglichst vollständige Risikoerfassung zu erhalten, sollten die Experten aus allen Unternehmensbereichen interviewt werden. Experteninterviews sind meist sehr effektiv bei der Kollektivierung von Risiken. Dennoch ist es gut noch weitere Methoden zu ergänzen, da auch die Experten nicht an alle Risiken denken können (vgl. Romeike 2018, S. 67 ff.).

Die Henkel AG & Co. KGaA beispielsweise kombiniert verschiedene Methoden in der Praxis miteinander. So wird die Risikoidentifizierung unter anderem mittels Checklisten durchgeführt, deren Inhalt im Laufe der Jahre weiterentwickelt und um immer neue Risiken ergänzt werden. Die Checklisten werden an die jeweiligen Experten in den unterschiedlichen Unternehmensbereichen verteilt und von ihnen auch durchgearbeitet. Den-

noch möchte sich das Unternehmen nicht nur auf die bereits aus der Vergangenheit bekannten Risiken konzentrieren, sondern hat für jeden Bereich auch freie Felder in den Checklisten vorgesehen. Damit sind die Experten aufgefordert, wie in einem Experteninterview, neue Denkanstöße zu geben und neue, noch nicht in der Checkliste enthaltene Risiken zu ermitteln (vgl. Henkel AG & Co. KGaA 2018, S. 107 f.).

Analytische Methoden

Analytische Methoden sind Suchmethoden mit einem eher strukturierten Charakter, wie zum Beispiel Abweichungsanalysen oder Trendanalysen.

Bei **Abweichungsanalysen** wird die Abweichung zwischen zwei Werten als mögliches Risiko betrachtet. Untersucht werden beispielsweise die Abweichung der Ist-Werten von den Plan-Werten oder die Abweichung zu Vorjahreswerten. Die Werte sind meistens Kennzahlen, wie zum Beispiel der Return-on-Equity. Ziel dieser Analyse ist es Risikofaktoren und Fehlentwicklungen in Kennzahlen zu erkennen und damit Risiken zu identifizieren (vgl. Rohlfs 2018, S. 120 f.).

Auch bei den **Trendanalysen** werden als Ausgangsbasis Kennzahlen oder andere Daten zu Sachverhalten beobachtet. Dies wird jedoch nicht nur zu zwei bestimmten Zeitpunkten gemacht, sondern über mehrere Zeitpunkte oder gesamte Zeiträume hinweg. Die Daten werden dann zu Zeitreihen verdichtet und nach erkennbaren Trends untersucht. Ist ein Trend gefunden, wird durch Extrapolation die Zukunft so weiterentwickelt, wie sich der Trend noch über einen gewissen Zeitraum lang fortsetzen würde. Sowohl der unterstellte Trend als auch die Folgen eines Trends können für ein Unternehmen mögliche Risiken darstellen. Wichtig ist, die Prognosezeiträume in die Zukunft relativ kurz zu halten, da Prognosen immer ungenauer werden, je weiter sie vom Aufstellungszeitpunkt entfernt sind (vgl. Rohlfs 2018, S. 122 f.).

Kreativitätstechniken

Kreativitätstechniken zeichnen sich dadurch aus, dass sie eher unstrukturiert und intuitiv an die Aufdeckung von neuen Risiken herangehen. Als Beispiele sind hier Brainstorming, Brainwriting oder Szenariotechniken zu nennen.

Das Ziel beim **Brainstorming** ist es innerhalb einer sehr kurzen Zeit möglichst viele Risiken zu identifizieren. Dabei kommt eine Gruppe aus mehreren Personen mit einem Moderator zusammen. Die Gruppe sollte nicht zu groß sein, da sonst die Gefahr von Störungen besteht, aber auch nicht zu klein sein, da sonst das Potenzial für den Ideenfluss zu gering ist. Wichtig ist auch, dass die Gruppe möglichst heterogen hinsichtlich ihrer Aufgaben im Unternehmen ist. Die Gruppenteilnehmer beginnen nun mögliche Risiken verbal zu nennen. Es sollen möglichst viele Risiken genannt werden, wobei auch unsinnige Ideen erlaubt sind. Eine Bewertung der Wortbeiträge oder Reaktionen auf Ideen anderer ist nicht erlaubt. Der Moderator dient dazu, den Ideenfluss zum Beispiel durch den Einwurf von Fragen aufrecht zu erhalten. Außerdem soll er die genannten möglichen Risiken schriftlich festhalten. Der Nachteil dieser Methode ist, dass die Teilnehmer sich unterbewusst gegenseitig in ihren Ideen beeinflussen (vgl. Romeike 2018, S. 127 ff.).

Das **Brainwriting** ist dem Brainstorming relativ ähnlich, da auch hier eine mittelgroße, heterogene Gruppe zusammenkommt und in sehr kurzer Zeit möglichst viele Risiken identifizieren möchte. Jedoch wird hier kein Moderator benötigt und es kommt auch zu keinem verbalen Austausch, da die Teilnehmer ihre Ideen zu möglichen Risiken zunächst schriftlich für sich selbst formulieren. Hier sind auch auf den ersten Blick unsinnig erscheinende Ideen erlaubt und um eventuelle Hemmschwellen von Teilnehmern kreativ zu denken zu überwinden, werden die Zettel anonymisiert. Als Hilfsmittel für die Teilnehmer zum Finden von Risiken können beispielsweise eine Risikomatrix oder eine Top-10-Risikotabelle dienen. Am Ende findet dann eine Diskussion der Teilnehmer über die erfassten Risiken statt. Der Vorteil dieser Methode ist, dass die Teilnehmer während ihrer Ideenfindung nicht durch die anderen Teilnehmer beeinflusst werden (vgl. Romeike 2018, S. 131 f.).

Bei **Szenariotechniken** geht es um die Risikoidentifizierung aus systematisch nachvollziehbaren Zukunftsbildern heraus. Zunächst wird eine Thematik rausgesucht, die mittels der Szenariotechnik näher untersucht werden soll. Rund um diese Thematik werden dann alle aktuellen erwägbaren Entwicklungen, beispielsweise in der Wirtschaft oder Gesellschaft, zusammengetragen. Aus den vorliegenden Daten werden im Anschluss nicht allzu realitätsferne Entwicklungen für die Zukunft prognostiziert. Dabei gehen Szenariotechniken einen Schritt weiter als Trendanalysen, da nicht nur erkennbare Trends fortgeführt, sondern auch Extremzonen entwickelt werden. Dadurch können sowohl absehbare Risiken als auch Risiken identifiziert werden, die erst in Extremsituationen entstehen würden, aber durchaus möglich sind und damit ebenfalls eine Gefahr für das Unternehmen darstellen können (vgl. Rohlfs 2018, S. 124).

2.3 Risikoklassifizierung

Als nächstes folgt die Risikoklassifizierung. Hierbei werden gleichartige Risiken vorher festgelegten Klassen zugeordnet. Unter gleichartigen Risiken werden in diesem Kapitel Risiken verstanden, die gemeinsame Charakteristika aufweisen.

Die Risikoklassifizierung bildet mit ihrer Aufbereitung der zuvor identifizierten Risiken die Grundlage der nachfolgenden Prozessschritte. Bei der Risikobewertung hilft eine vorherige Klassifizierung zum einen, weil gleichartige Risiken bei der Risikobewertung auch gleichen Bewertungsgrundsätzen unterliegen. Zum anderen dienen Risikoklassen dazu Diversifikationseffekte im Rahmen der Bewertung der Risikotragfähigkeit eines gesamten Unternehmens zu bestimmen (vgl. Siemens und Dahms 2014, S. 29). Bei der Risikosteuerung hilft eine vorherige Klassifizierung bei dem Einsatz zielgerichteter Maßnahmen gegen die Risiken und bei der Risikoberichterstattung helfen Risikoklassen dabei, die Kommunikation und die Berichte über die Unternehmensrisiken strukturierter darzustellen (vgl. Rohlfs 2018, S. 125).

Wenn es bei der Risikoklassifizierung unter anderem darum geht, bei einer strukturierten Risikoberichterstattung zu unterstützen, ist anzunehmen, dass durch gesetzliche Stan-

dards geregelt wird, in welche Klassen ein Unternehmen Risiken einzuteilen hat. Unter dem Aspekt der Übersichtlichkeit für die Leser von Risikoberichten verschiedener Unternehmen, wären einheitliche Klassen durchaus verständlich. Tatsächlich gibt es keine gesetzlichen Standards. Der DRS 20 formuliert sogar explizit, dass die Risikoklassen vom Unternehmen individuell gewählt werden können. Für Unternehmen, die keine individuellen Klassen bilden wollen, wird lediglich der Vorschlag geäußert, die Risiken in folgende Klassen einzuordnen: Umfeld-, Branchen-, leistungswirtschaftliche, finanzwirtschaftliche und sonstige Risiken (vgl. DRS 2012, Tz. 164).

Hat ein Unternehmen für sich individuelle Risikoklassen festgelegt, müssen die vorher identifizierten Risiken diesen Klassen zugeordnet werden. Die Zuordnung kann dabei auf verschiedene Weisen erfolgen. Zum einen kann ein Unternehmen Risiken danach zuordnen wie lang die Fristigkeit der zugrunde liegenden Managemententscheidung ist. Steht ein Risiko beispielsweise mit einer sehr langfristig bindenden Entscheidung in Zusammenhang, würde das Risiko der Klasse der strategischen Risiken zugeordnet werden, ist die Entscheidung eher kurzfristig bindend würde das Risiko eher der Klasse der operativen Risiken zugeordnet werden. Zum anderen kann ein Unternehmen die Zuordnung auch nach den Auswirkungen auf bestimmte Unternehmensziele oder -bereiche vornehmen. Demnach würden alle Risiken, die sich auf die Strategie auswirken, den strategischen Risiken zugeordnet werden und alle Risiken, die sich auf das operative Geschäft des Unternehmens auswirken, den operativen Risiken zugeordnet werden. Da manche Risiken sich jedoch auf ganz unterschiedliche Bereiche auswirken können, müsste bei dieser Zuordnung klar geregelt sein, wie die Klasse ausgewählt wird, auf die ein Risiko sich am stärksten auswirkt. Ein Risiko sollte immer nur einer Klasse zugeordnet werden. Eine Zuordnung nach der Risikoquelle bzw. -ursache ist in dieser Hinsicht eindeutiger. Hierbei werden Risiken, die im operativen Geschäft entstehen den operativen Risiken zugeordnet, während Risiken, die sich aus der Unternehmensstrategie ergeben, den strategischen Risiken zugeordnet werden (vgl. Diederichs 2018, S. 97).

Hilfreich für die Risikoklassifizierung ist, wenn bei der Risikoidentifizierung Priorität auf die Anforderung der Konsistenz von Risiken gelegt wurde. Denn wurden Risiken möglichst eindeutig und überschneidungsfrei erfasst, können sie leichter den Klassen zugeordnet werden. Außerdem ist es wichtig, dass ein Unternehmen bei der Klassenbildung klar definiert, was unter der jeweiligen Klasse verstanden wird. Denn wenn alle Mitarbeiter ein einheitliches Verständnis von den Bedeutungen der Klassen haben, können sie eine eindeutige Zuordnung der Risiken vornehmen.

2.3.1 Praxisbeispiel: Risikoklassifizierung bei der Henkel AG & Co. KGaA

Da jedes Unternehmen eine individuelle Risikoklassifizierung durchführen kann und es keine idealtypischen Klassen gibt, soll im Folgenden anhand eines Beispiels gezeigt werden, wie eine Klassifizierung von Risiken in der Praxis konkret aussehen könnte.

Die Henkel AG & Co. KGaA hat die Risikoklassen angelehnt an die eigene Unternehmensstruktur gebildet. Dabei werden die Klassen wie in Abb. 2.5 dargestellt definiert.

Zunächst werden alle Risiken in operative, funktionale und unternehmensstrategische Risiken gegliedert. Unter operativen Risiken werden Risiken verstanden, die im Zusammenhang mit relativ kurzfristig bindenden Entscheidungen stehen und sich aus den Unternehmensaktivitäten im Markt anhand der Wertschöpfungskette des Unternehmens ergeben. Risiken, welche den funktionalen Risiken zugeordnet werden können, stehen ebenfalls im Zusammenhang mit relativ kurzfristig bindenden Entscheidungen, ergeben sich jedoch aus den Bereichen oder Funktionen, welche nur unterstützende Unternehmensaktivitäten durchführen und damit der Wertschöpfungskette des Unternehmens nur zuarbeiten. Zu den **unternehmensstrategischen Risiken** lassen sich alle Risiken zuordnen, welche im Zusammenhang mit langfristig bindenden Entscheidungen stehen. Unter langfristig bindenden Entscheidungen versteht das Unternehmen Investitionsentscheidungen im Sinne der Unternehmensstrategie, wie beispielsweise interne Projekte, Akquisitionen und strategische Kooperationen. Unternehmensstrategische Risiken sind demnach zum Beispiel Ereignisse, die Projekte verzögern oder gar stoppen könnten, oder andere Ereignisse, die dafür sorgen, dass die Erwartungen in die getroffenen langfristig bindenden Entscheidungen nicht erfüllt werden (vgl. Henkel AG & Co. KGaA 2018, S. 110, 116).

Die **operativen Risiken** lassen sich weiter in drei Risikoklassen gliedern: Die Beschaffungsmarktrisiken, die Produktionsrisiken und die Umfeld- und Branchenrisiken. Hierbei ist zu erwähnen, dass die Umfeld- und Branchenrisiken die Absatzrisiken mit beinhalten.



Abb. 2.5 Risikoklassen der Henkel AG & Co. KGaA. (Quelle: eigene Darstellung in Anlehnung an Henkel AG & Co. KGaA 2018, S. 110)

Damit spiegeln diese drei Risikoklassen die drei Schritte der Wertschöpfungskette eines produzierenden Unternehmens wie Henkel wider. Als Erklärung dafür, was unter den einzelnen Klassen verstanden wird, hat Henkel in seinem Geschäftsbericht für jede der Klassen Beispiele für mögliche Risiken genannt, welche in die jeweilige Klasse eingeordnet werden können. So werden der Klasse **Beschaffungsmarktrisiken** alle Risiken zugeordnet, die bei der Beschaffung von Materialien auftreten können. Dazu gehören Preisrisiken, die durch steigende Materialpreise entstehen, aber auch Lieferrisiken, wie Lieferengpässe bei den Lieferanten. Unter **Produktionsrisiken** fallen alle Risiken, die während der Produktion von Gütern auftreten können, wie beispielsweise ungeplante Betriebsunterbrechungen oder zu niedrige Kapazitätsauslastungen infolge von Volumenrückgängen. Zu der Klasse **Umfeld- und Branchenrisiken** lassen sich alle Risiken zuordnen, die in der Branche des betrachteten Unternehmens und dessen Umfeld, also auf dem Absatzmarkt des Unternehmens auftauchen. Dazu gehört beispielsweise die Zunahme von Konfliktherden als geopolitisches Risiko oder eine mögliche Abschwächung der Konjunktur durch den Brexit, aber auch globale Handelskonflikte oder eine Verschlechterung des Konsumklimas können dieser Risikoklasse zugeordnet werden. Ein wesentliches Risiko in dieser Klasse ist der Anstieg des Promotions- und Preisdrucks, der in der Branche durch Wettbewerbsintensivierung entsteht (vgl. Henkel AG & Co. KGaA 2018, S. 110 ff.).

Auch die **funktionalen Risiken** lassen sich weiter in sechs Zuständigkeitsbereiche untergliedern, die unterstützende Funktionen zum operativen Geschäft darstellen. Der erste Zuständigkeitsbereich, kümmert sich um die Finanzen, sodass hierunter alle finanzwirtschaftlichen Risiken fallen. Da Finanzen ein großer Bereich ist, werden innerhalb dieses Bereiches fünf Risikoklassen gebildet, in die die finanzwirtschaftlichen Risiken eingeordnet werden können (vgl. Henkel AG & Co. KGaA 2018, S. 110).

In die Klasse **Ausfallrisiken** werden alle Risiken einsortiert, die daraus entstehen, dass eine Vertragspartei, mit der Henkel einen Vertrag geschlossen hat, ihre Verpflichtungen gegenüber Henkel nicht erfüllen kann. Darunter fallen zum Beispiel Kunden, die ihre Rechnungen für gelieferte Produkte nicht bezahlen, oder Unternehmen, von denen Henkel Wertpapiere erworben hat, die Zinsen oder Rückzahlungsbeträge nicht mehr aufbringen können (vgl. Henkel AG & Co. KGaA 2018, S. 192 ff.). Den **Liquiditätsrisiken** werden alle Risiken zugeordnet, die darauf beruhen, dass Henkel selbst nicht jederzeit seinen Verpflichtungen gegenüber anderen nachkommen kann. Dies könnte zum Beispiel passieren, wenn zu viel Geld in Finanzinstrumenten mit langen Laufzeiten gebunden ist (vgl. Henkel AG & Co. KGaA 2018, S. 196). Unter **Währungsrisiken** sind alle Risiken zu verstehen, die aus Wertänderungen von künftigen Fremdwährungszahlungen infolge von Wechselkursschwankungen resultieren. Dies wäre beispielsweise der Fall, wenn es bei der Produktion eines Produktes in einem Land und dem Verkauf dieses Produktes in einem anderen Land durch Wechselkursschwankungen zu Verlusten kommt. Den **Zinsrisiken** werden alle Risiken zugeordnet, welche sich aus veränderten Zinsen ergeben. Zwei Beispiele für Zinsrisiken sind das Fair-Value-Risiko, bei dem durch Zinsänderungen die Zeitwerte von festverzinslichen Wertpapieren schwanken, und das Cashflow-Risiko, bei dem durch Zinsänderungen die Zinszahlungen von variabel verzinslichen Wertpapieren schwanken (vgl.

Henkel AG & Co. KGaA [2018](#), S. 198 ff.). Die letzte Risikoklasse der finanzwirtschaftlichen Risiken heißt **Risiken aus Pensionsverpflichtungen** und hierunter werden alle Risiken verstanden, die aus den Pensionsverpflichtungen entstehen, welche Henkel ihren Mitarbeitern zugesichert hat. Dazu gehören zum Beispiel Langlebigkeitsrisiken, da Pensionsverpflichtungen lebenslange Leistungen enthalten, oder die Inflation (vgl. Henkel AG & Co. KGaA [2018](#), S. 170 f.).

Neben dem Bereich der Finanzen gibt es noch fünf andere Bereiche, die auch gleichzeitig eine jeweilige Risikoklasse darstellen. Somit gibt es noch die Klasse **Rechtliche Risiken**, in die alle Risiken eingeordnet werden, welche im Zusammenhang mit Rechtsstreitigkeiten oder behördlichen Verfahren entstehen. Solche Risiken können zum Beispiel Produktfehler, Schutzrechtverletzungen, die falsche Sanierung von Altlasten oder Verstöße gegen den Umweltschutz sein, welche rechtliche oder behördliche Verfahren nach sich ziehen. Auch Streitigkeiten im Patent- oder Steuerrecht gehören dazu. Neben den rechtlichen Verfahren sind weiterhin auch noch Risiken dieser Klasse zuzuordnen, welche im Zusammenhang mit Veränderungen im regulatorischen Umfeld des Unternehmens entstehen. Regulatorische Risiken, wie zum Beispiel Import- und Exportkontrollen, Zollbestimmungen, Preis- und Währungsbeschränkungen oder andere Regulierungen im Handel, sind damit auch den rechtlichen Risiken zuzuordnen (vgl. Henkel AG & Co. KGaA [2018](#), S. 113).

Der Klasse **Informationstechnische Risiken** (IT-Risiken) sind diejenigen Risiken zuzuordnen, die im Zusammenhang mit unternehmensinternen und -externen IT-Diensten, den Applikationen und Netzwerken des Unternehmens und seinem Infrauktursystem entstehen. Dazu gehören beispielsweise, dass es zu einer Manipulation oder einem Verlust von wichtigen Daten kommt oder relevante IT-Dienste ausfallen oder gestört sind (vgl. Henkel AG & Co. KGaA [2018](#), S. 114).

Risiken, die im Zusammenhang mit der Akquisition und dem Binden von Mitarbeitern aufkommen, lassen sich der Klasse **Personalrisiken** zuordnen. Darunter fallen Risiken wie etwa der Verlust von wertvollen Mitarbeitern des Unternehmens oder die Nichtgewinnung von dringend benötigten Fachkräften. Risiken, wie zum Beispiel der Reputationsverlust oder ein Imageschaden der Unternehmensmarke, sind hingegen in die Klasse **Risiken in Verbindung mit Markenimage oder Ruf des Unternehmens** einzuordnen (vgl. Henkel AG & Co. KGaA [2018](#), S. 115).

Die letzte Risikoklasse, welche Henkel bildet, ist die der **Umwelt- und Sicherheitsrisiken**. Hierunter fallen alle Risiken, die im Bereich Umwelt und Sicherheit entstehen. Oft haben diese Risiken, wie beispielsweise Bodenkontaminationen oder Leckagen, Auswirkungen auf die Gesundheit von Menschen und Tieren (vgl. Henkel AG & Co. KGaA [2018](#), S. 116).

Anhand der Beschreibungen der Risikoklassen, welche die Henkel AG & Co. KGaA in ihrem Geschäftsbericht vorgenommen hat, lässt sich erkennen, dass die Zuordnung der Risiken in die jeweiligen Klassen hauptsächlich aufgrund der Lokalisierung der Risikoquelle stattgefunden hat. Lieferengpässe bei den Lieferanten wichtiger Materialien zum Beispiel haben auch Auswirkungen auf die Produktion eines Unternehmens, wurden je-

doch den Beschaffungsmarktrisiken zugeordnet, weil die Risikoquelle im Beschaffungs- markt liegt. Allerdings hat Henkel auch nach der Fristigkeit der zugrunde liegenden Managemententscheidung unterschieden, was daran zu erkennen ist, dass die Risiken im Zusammenhang mit langfristig bindenden Entscheidungen von den anderen gänzlich getrennt wurden und in die Klasse unternehmensstrategische Risiken eingeordnet wurden.

2.3.1.1 Vergleich mit der Risikoklassifizierung des DRS 20

Während die Henkel AG & Co. KGaA vierzehn einzelne Risikoklassen gebildet hat, wurden im Vorschlag des DRS 20 lediglich fünf Risikoklassen genannt. Im DRS20 wurde zwar nicht erklärt, welche Risiken den fünf Klassen genau zuzuordnen sind, jedoch lassen sich diese Klassen relativ gut interpretieren.

Die Klasse der leistungswirtschaftlichen Risiken im DRS 20 könnte man mit den operativen Risiken von Henkel gleichsetzen, da dort der Prozess entlang der Wertschöpfungskette des Unternehmens abgebildet wird. Henkel differenziert diesen Prozess noch weiter in drei verschiedene Risikoklassen. Des Weiteren hat Henkel die Umfeld- und Branchenrisiken eher dem Absatzmarkt zugeordnet, indem es diese Risiken den operativen Risiken zuordnet. Der DRS 20 hingegen hat den Absatzmarkt diesen Risiken nicht zugeordnet und unabhängig von den leistungswirtschaftlichen Risiken je eine separate Klasse aus Umfeld- und Branchenrisiken definiert. Hierbei bleibt die Frage offen, wie der DRS 20 die Bedeutung der Begriffe „Umfeld“ und „Branche“ voneinander trennt.

Sowohl Henkel als auch der DRS 20 haben die finanzwirtschaftlichen Risiken von den anderen Risiken getrennt. Weiterhin fällt auf, dass Henkel noch viele weitere Risikoklassen unterscheidet, jedoch im Gegensatz zum DRS 20 keine Risikoklasse hat, welche „sonstige Risiken“ erfasst. Dies bedeutet, dass jedes Risiko, welches bei der Risikoidentifizierung aufgedeckt wird, zwingend einer der vierzehn Risikoklassen zugeordnet werden muss. Bestehen Unsicherheiten dabei, zu welcher Risikoklasse ein Risiko nun gehört, muss sich letztendlich doch auf eine der Risikoklassen geeinigt werden. Gerade deswegen ist es umso wichtiger, dass die Risikoklassen vom Unternehmen eindeutig und überschneidungsfrei beschrieben werden und ein einheitliches Verständnis über die Klassen besteht.

2.3.1.2 Risikointerdependenzen

Bei der Risikoklassifizierung von Henkel wurden die Risiken den vorher definierten Klassen danach zugeordnet, in welchem Unternehmensbereich sich ihre Risikoquelle befindet. Es sollte jedoch niemals außer Acht gelassen werden, dass die einzelnen Risiken auch aus anderen Risiken entstehen können. Beispielsweise würde das Risiko, dass ein Unternehmen ein Produkt nicht auf dem Markt verkauft bekommt, der Risikoklasse Umfeld- und Branchenrisiken zugeordnet werden, da das Risiko auf dem Absatzmarkt entsteht. Allerdings könnte der Grund dafür, dass das Produkt nicht abgesetzt werden kann, auch ein Produktionsfehler sein. Das Absatzrisiko entsteht zwar erst auf dem Absatzmarkt, wurde aber durch das Risiko Produktionsfehler ausgelöst. Gleichzeitig kann sich ein Risiko aus dem Absatzmarkt, wie etwas sinkende Absatzzahlen, auch auf ein Risiko aus der Klasse Produktionsrisiken, wie beispielsweise dem Risiko der zu niedrigen Kapazitätsauslastung,

gen infolge von Volumenrückgängen, auswirken. Ein Unternehmen sollte sich diesen Zusammenhängen zwischen den einzelnen Risiken auch klassenübergreifend in den folgenden Prozessschritten des Risikomanagementprozesses bewusst sein. Die Risikoklassifizierung soll lediglich der Strukturiertheit und der Vereinfachung von zukünftigen Prozessschritten dienen und keinesfalls für die fälschliche Annahme sorgen, dass die Risiken aus unterschiedlichen Klassen nichts miteinander zu tun hätten (vgl. Diederichs 2018, S. 102).

2.3.2 Weitere Systematisierung der Risiken

Hat ein Unternehmen individuelle Risikoklassen gebildet und die zuvor identifizierten Risiken diesen Klassen eindeutig zugeordnet, kann bei Bedarf die Risiken innerhalb der Klassen nach bestimmten Kriterien noch weiter systematisiert werden. Dabei sind Risiken nach allen möglichen Kriterien zu gliedern, wie zum Beispiel nach der Wirkungsweise von Risiken. Dabei wird unterschieden, ob ein Risiko direkte Schäden verursacht und damit zu einer unmittelbaren Beeinträchtigung führt, welche auch messbar ist, oder ob es indirekte Schäden verursacht und damit zu einer mittelbaren Beeinträchtigung führt, welche lediglich schätzbar ist. Eine Betriebsunterbrechung wäre beispielsweise ein direktes Risiko, während der Verlust von wertvollen Mitarbeitern eher zu indirekten Risiken zählt. Eine andere Unterteilung könnte nach der Messbarkeit von Risiken erfolgen. Hierbei wird unterschieden zwischen quantitativen Risiken, deren Auswirkungen durch Kennzahlen bewertbar sind, und qualitativen Risiken, deren Auswirkungen nicht direkt bewertbar sind. Zinsrisiken, wie etwa das Fair-Value-Risiko, zählen zu den quantitativen Risiken, während Reputationsrisiken eher qualitative Risiken darstellen (vgl. Rohlfs 2018, S. 15).

Eine Systematisierung muss nicht zwingend durchgeführt werden. Sie kann jedoch hilfreich sein, je nach dem aus welcher Perspektive Risiken betrachtet werden und welche Informationen über Risiken benötigt werden. Für eine Versicherungsabteilung eines Unternehmens kann es zum Beispiel durchaus interessant sein, zu wissen, auf welche Risiken sie mit ihrer Arbeit Einfluss nehmen kann. Um dies zu beantworten, kann eine Systematisierung dahingehend durchgeführt werden, ob ein Risiko versicherbar oder nicht versicherbar ist.

Unter Berücksichtigung der zuvor erläuterten Risikoklassifizierung der Henkel AG & Co. KGaA und den bereits genannten Risikobeispielen für die jeweiligen Klassen, werden diese Risiken nun einmal zur Veranschaulichung nach ihrer Versicherbarkeit systematisiert:

Aus der Klasse Beschaffungsmarktrisiken sind mögliche steigende Marktpreise von zu beschaffenden Materialen und Lieferengpässe von Lieferanten nicht versicherbar. Ungeplante Betriebsunterbrechungen aus der Klasse Produktionsrisiken sind jedoch im Rahmen einer Betriebsunterbrechungsversicherung versicherbar. Als weiteres Beispiel der Produktionsrisiken wurden Volumenrückgänge genannt, welche nicht versicherbar sind. Genauso wenig versicherbar sind die unter Umfeld- und Branchenrisiken genannten Bei-

spiele: Zunahme von Konfliktherden, Abschwächung der Konjunktur, globale Handelskonflikte, zunehmender Druck durch steigende Wettbewerbsintensität und Verschlechterung des Konsumklimas. Die Beispiele, welche unter den finanzwirtschaftlichen Risiken genannt wurden, wie Wechselkursschwankungen oder Zinsänderungen, sind mit Ausnahme der Risiken aus Pensionsverpflichtungen alle nicht versicherbar. Risiken in der Klasse rechtliche Risiken sind größtenteils versicherbar. Hier kommen Versicherungen wie die Rechtsschutzversicherung beim Beginnen eines Rechtsstreits und die Haftpflichtversicherung beim gerichtlichen Abwehren von unberechtigten Schadenersatzansprüchen in Frage. So können Produktfehler auch über die Produkthaftpflichtversicherung, Verstöße gegen den Umweltschutz über die Umwelthaftpflichtversicherung und Streit im Patent- und Steuerrecht über die Patentrechtschutz- und Steuerrechtschutzversicherung versichert werden. Die regulatorischen Risiken in der Klasse der rechtlichen Risiken sind jedoch nicht versicherbar. In der Klasse der informationstechnischen Risiken können Manipulation und Verlust von Daten oder Ausfall und Störung von IT-Systemen über die Cyberversicherung versichert werden. Bei einer Manipulation von Daten oder IT-Systemen durch eigene Mitarbeiter ist die Vertrauensschadenversicherung die passende Absicherung. Die Risiken in den Klassen Personalrisiken sind hingegen in der Regel nicht versicherbar. Durch auf dem Markt existierende Reputationsschaden-Versicherungen sind Risiken in Verbindung mit Markenimage oder Ruf des Unternehmens versicherbar. Risiken aus der Klasse der Umwelt- und Sicherheitsrisiken sind zum Teil versicherbar. Wenn es sich beispielsweise um Bodenkontaminationen oder Leckagen handelt, dann können diese Risiken über eine Umweltschadenversicherung versichert werden.

2.4 Ergebnis der Risikoidentifizierung und -klassifizierung

Das Ergebnis des ersten Schrittes im Risikomanagementprozess ist eine strukturierte Darstellung der Informationen, welche man bei der Risikoidentifizierung und -klassifizierung erhalten hat. Dabei gibt es zwei Darstellungsformen, die man wählen kann.

Zum einen besteht die Möglichkeit einer grafischen Darstellung aller Informationen, indem eine sogenannte Risikolandschaft erstellt wird. Dabei handelt es sich um eine Grafik in Form einer Art Mind-Map, welche alle bestehenden und potenziellen identifizierten Risiken, zugeordnet zu ihren jeweiligen Risikoklassen, enthält. Diese kann aussehen wie in Abb. 2.6 dargestellt.

Zum anderen kann ein Unternehmen die Informationen auch in einer listenartigen Darstellung abbilden. Diese Art der Darstellung wird Risikokatalog genannt. Hierbei werden alle bestehenden und potenziellen identifizierten Risiken, zugeordnet zu ihren jeweiligen Risikoklassen, untereinander in einer Spalte aufgelistet. In den anderen Spalten der Liste werden hier noch die jeweiligen Charakteristika der Risiken beschrieben (vgl. Rohlfs 2018, S. 101 f.).

Durch ergänzende Spalten mit weiteren Charakteristika der Risiken ist der Risikokatalog umfangreicher als die Risikolandschaft. Somit sollte der Risikokatalog zwingend er-

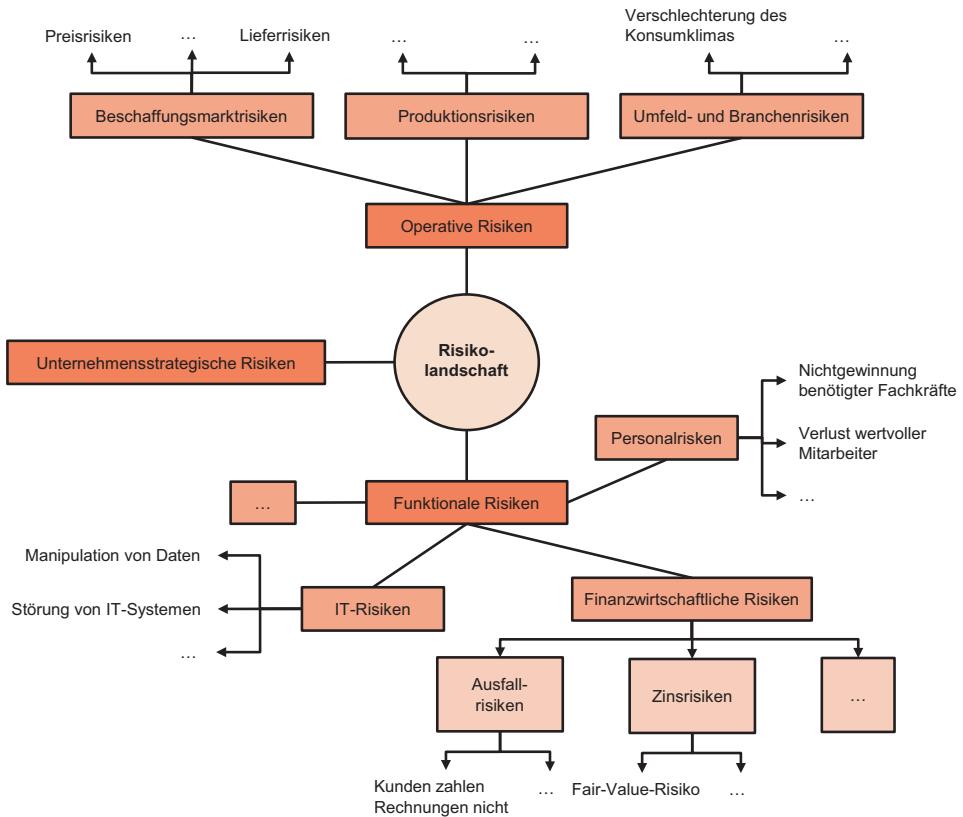


Abb. 2.6 Risikolandschaft. (Quelle: eigene Darstellung in Anlehnung an Rohlfs 2018, S. 101)

stellt werden, die Risikolandschaft dagegen dient im Rahmen der Berichterstattung eher der Veranschaulichung.

Literatur

- Deutsches Institut für Normung e. V. (2010). *Risikomanagement – Verfahren zur Risikobeurteilung (IEC/ISO 31010:2009)*. Berlin: Beuth.
- Deutsches Rechnungslegungs Standards Committee (DRS20). (2012). Deutscher Rechnungslegungsstandard Nr.20 (DRS 20): Konzernlagebericht, 19. Öffentliche Sitzung, 14.09.2012.
- Diederichs, M. (2018). *Risikomanagement und Risikocontrolling*. München: Franz Vahlen.
- Henkel AG & Co. KGaA. (2018). Henkel Geschäftsbericht 2018. Düsseldorf.
- Rohlfs, T. (2018). *Risikomanagement im Versicherungsunternehmen* (2. Aufl.). Karlsruhe: Versicherungswirtschaft.
- Romeike, F. (2018). *Risikomanagement*. Wiesbaden: Springer Gabler.
- Rosenkranz, F., & Missler-Behr, M. (2005). *Unternehmensrisiken erkennen und managen – Einführung in die quantitative Planung*. Berlin/Heidelberg: Springer.

- Sartor, F. J., & Bourauel, C. (2013). *Risikomanagement kompakt. In 7 Schritten zum aggregierten Nettorisiko des Unternehmens*. München: Oldenbourg Wissenschaftsverlag GmbH.
- Siemens, A., & Dahms, S. (2014). *Risikomanagement kompakt – Lektion 3 – Werkzeuge im Risikokreislauf: Identifikation, Bewertung, Aggregation*. Eschborn: Management Circle.

Wolfgang Knauf ist seit 2014 als Corporate Director Insurance für den Versicherungsbereich bei Henkel AG & Co. KGaA verantwortlich. In die Zuständigkeit der Versicherungsabteilung fällt unter anderem die Platzierung und Koordination aller globalen Versicherungsprogramme des Henkel Konzerns. Vor seiner Tätigkeit bei Henkel war er über 30 Jahre bei einem der weltweit großen internationalen Versicherungsmakler zuletzt im Strategic Account Management tätig.

Jessica Bender absolvierte im dualen System bei der Gothaer Versicherung das Bachelorstudium „Versicherungswesen“ am Institut für Versicherungswesen der Technischen Hochschule Köln. Ihre Schwerpunkte waren dabei Haftpflicht-, Unfall-, Kraftfahrt- und Rechtsschutzversicherung, Personalmanagement und Organisations- und Informationsvermittlung. An der TH Köln absolvierte sie im Anschluss auch das Masterstudium „Risk & Insurance“ und arbeitete währenddessen im Vertriebsmanagement der Gothaer.



Risikoanalyse, -bewertung und -steuerung

3

Alexander Skorna und Philipp Nießen

Zusammenfassung

Unternehmen müssen sich mit ihren Risiken befassen und diese nach der Identifikation analysieren, bewerten und steuern. Das Kapitel befasst sich mit diesen Elementen im Risikomanagement. Im Vorhinein werden Risiken in Industrieunternehmen kurz angerissen und das Prinzip von Ursache und deren Wirkung beschrieben. Die Risikoanalyse beschreibt verschiedene Analysemethoden, um die Beschaffenheiten der Risiken darzustellen. Die Bewertung setzt sich mit den verschiedenen Methoden und Klassifizierungen der analysierten Risiken auseinander. Das letzte Kapitel, der Risikobewältigungsmix, ist aufgegliedert nach ursachen- und wirkungsbezogenen Methoden. Die ursachenbezogenen Methoden beschreiben die Vermeidung und Verminderung von Risiken, die wirkungsbezogenen Methoden setzen sich mit der Verlagerung und der Akzeptanz der Risiken auseinander. Somit wird in diesem Kapitel ein allumfassender Überblick über den Umgang mit Unternehmensrisiken gegeben.

A. Skorna (✉)

Funk Versicherungsmakler GmbH, Hamburg, Deutschland

E-Mail: a.skorna@funk-gruppe.de

P. Nießen

TH Köln, Institut für Versicherungswesen, Köln, Deutschland

E-Mail: philippniessen@web.de

3.1 Einleitung

Um zuvor identifizierte Risiken besser für das Unternehmen darzustellen, werden die Risiken genauer analysiert, anschließend bewertet und im letzten Schritt gesteuert. In diesem Kapitel werden diese drei Prozesse genauer erklärt und auf die verschiedenen Möglichkeiten eingegangen.

Zur Analyse, Bewertung und Steuerung von Risiken, müssen der Risikobegriff im Sinne eines Grundverständnisses systematisiert und die verschiedenen Betrachtungsweisen dargestellt werden. Das Risiko wird in der Literatur meist als die mögliche positive oder negative Abweichung eines Ereignisses von dem erwarteten Ereignis verstanden (vgl. Gleißner 2017, S. 16). Oftmals wird der Begriff auch als ein Zusammenspiel von Ursache und Wirkung und der daraus resultierenden Unsicherheit von Entscheidungen definiert. Die Gemeinsamkeiten der verschiedenen Definitionen liegen in der Unvollkommenheit der vorhandenen Informationen und der damit verbundenen negativen Abweichung definierter Unternehmensziele. Der Begriff wird in der Praxis häufig nur mit einer Gefahr verbunden, wohingegen das Risiko auch positiv sein kann und somit auch als Chance angesehen werden kann. Falls die Wahrscheinlichkeit eines eintretenden Schadens bei einer bekannten Anzahl an zukünftigen Situationen zwischen null und eins verteilt ist, kann man ein Risiko von Entscheidungen als eine Wahrscheinlichkeitsverteilung der Ereignisse auffassen. In diesem Fall spricht man von einer Entscheidung unter Risiko (vgl. Skorna 2013, S. 22 f.). Sind die verschiedenen Ergebnisse bekannt und die zugehörigen Wahrscheinlichkeiten können nur subjektiv geschätzt werden bzw. es können keine genauen Wahrscheinlichkeiten zugeordnet werden, spricht man von einer Entscheidung unter Unsicherheit (vgl. Gutenberg 1962, S. 78 f.). In der Praxis wird die ursachenbezogene Definition des Risikobegriffs erweitert. Da Unternehmen oft keine bestimmbareren Wahrscheinlichkeiten über alle Prozessabläufe darstellen können, werden Erfahrungswerte oder Durchschnittswerte als Hilfsgrößen in den Bewertungsprozess einbezogen. Der Begriff wird somit um eine wirkungsbezogene Definition erweitert. Dieser fokussiert sich auf die negativen Auswirkungen, welche sich aus dem Eintritt eines Risikos ergeben können. Das Eintreten eines ungünstigen Ausgangs, resultierend durch eine Fehlentscheidung, wird in diesem Fall als Risiko angesehen (vgl. Skorna 2013, S. 23).

Unternehmen müssen bewusst Risiken eingehen, um aus ihrem eingebrachten Kapital einen adäquaten Profit zu erzielen. Um diese Risiken abschätzen und steuern zu können, benötigen die Unternehmen einen gut geregelten und dokumentierten Risikomanagementprozess. Der Prozess verlangt ein unternehmensspezifisch ausgestalteten Risikostrategie (vgl. Rohlfs 2018, S. 73 ff.).

Die Einführung eines Risikomanagements wirkt sich wesentlich auf die Risikopolitik eines Unternehmens aus. Das Unternehmen erhält einen ganzheitlichen Überblick über alle Risiken innerhalb des Unternehmens und kann diese geeigneter abschätzen und steuern. Werden alle vorhandenen Risiken und die resultierenden Korrelationen erkannt und zielorientiert gesteuert, kann die Risikopolitik des Unternehmens stark beeinflusst wer-

den. Die Unternehmensleitung kann durch gutes Risikomanagement frühzeitig und vorausschauend Anpassungen vornehmen und muss nicht erst im Schadenfall angesichts eines finanziellen Verlusts agieren. Letztlich werden die Unternehmensziele durch die Implementierung des Risikomanagementprozesses stärker fokussiert (vgl. Hölscher et al. 2002, S. 207 f.).

3.2 Risikoanalyse

Die Risikoanalyse ist der erste Schritt nach der Identifizierung der Risiken. Es werden die vorhandenen Risiken überprüft und genauer betrachtet. Wichtig ist, dass die Risiken nicht nur einzeln betrachtet werden, sondern das Gesamtportfolio des Unternehmens stets im Blick ist und ganzheitlich analysiert wird.

3.2.1 Geschäftsrisiken und operationelle Risiken

Die größten Risiken in Unternehmen sind Geschäftsrisiken und operationelle Risiken. Unter Geschäftsrisiken verstehen sich Risiken, die von außen auf das jeweilige Unternehmen einwirken und eine negative bzw. positive Auswirkung auf das Unternehmen haben können. Für Deutschland und viele andere Länder zählt das Betriebsunterbrechungsrisiko zu den größten Geschäftsrisiken. An zweiter Stelle liegt das Cyberrisiko, welches in den letzten Jahren immer mehr Bedeutung erlangt. Dies ist auch darin zu erkennen das im Jahr 2020 Unternehmen eine Betriebsunterbrechung durch Cyberangriffe als größte Gefahr ansehen (vgl. AGCS 2020).

Operationelle Risiken beschreiben das Verlustrisiko, das sich aus der Unangemessenheit oder dem Versagen von internen Prozessen, Mitarbeitern oder Systemen oder durch externe Ereignisse ergibt (vgl. § 7 Nr. 24 VAG). Das große Problem bei der Analyse von operationellen Risiken liegt darin, dass jedes Unternehmen eigene spezifische Risiken aufweist. Normalerweise liegen auch für die Messung dieser Risiken keine externen historischen Daten vor, somit müssen eigene interne Daten aufgebaut werden. Somit bestehen operationelle Risiken aus Personen-, Prozess- und Systemrisiken. Unter Personenrisiken fallen nicht nur Risiken aus fehlerhaften Handlungen der Angestellten, sondern auch solche Risiken, welche aus fehlender Kommunikation, falschem Führungsverständnis, schlechtem Betriebsklima oder dem Ausfall von Personen resultieren. Unter Personenrisiko versteht man somit alle Risiken, welche unter Corporate Governance fallen. Als Prozessrisiken werden Risiken verstanden, die nicht in erster Linie aus Personen- und Systemrisiken resultieren. Es sind hauptsächlich Störungen, die den Geschäftsablauf aufgrund unvollständiger Ablaufbeschreibungen, Mängeln und der Aufbau- und Ablauforganisation und mangelnder Kontrollen unterbrechen. Systemrisiken sind Risiken, die sich aus Schäden aus der Nichtverfügbarkeit von IT-Systemen und Daten ergeben (vgl. Wolke 2009, S. 201 ff.).

Tab. 3.1 Checkliste zur Identifikation der wichtigsten Unternehmensrisiken

Bedrohung von Kernkompetenzen oder Wettbewerbsvorteilen	Wertschwankungen von Beteiligungen oder Wertpapieren des Umlaufvermögens
Risiken durch eine Unternehmensstrategie, die inkonsistent ist oder auf sehr unsicheren Planungsprämissen basiert	Risiken aus dem Einsatz von Derivaten
Strukturelle Risiken der Märkte infolge ungünstiger Struktur der Wettbewerbskräfte (z. B. geringe Differenzierungschancen in stagnierenden Märkten, niedrige Markteintrittshemmnisse oder erhebliche Substitutionsgefahr)	Organisatorische Risiken durch fehlende bzw. unklare Aufgaben- und Kompetenzregelung oder Schwächen des internen Kontrollsystems
Starke Abhängigkeiten von wenigen Kunden oder wenigen Lieferanten	Risiken durch den Ausfall von Schlüsselpersonen
Gemessen am Gesamtrisikoumfang zu niedrige oder infolge des geplanten Unternehmenswachstums tendenziell sinkende Eigenkapitalquote	Haftpflichtschäden oder Produkthaftpflichtfälle
Ausgeprägte (z. B. konjunkturelle oder saisonale) Nachfrageschwankungen (Preis oder Menge)	Beeinträchtigung der Lieferfähigkeit durch den Ausfall zentraler Komponenten der Produktion
Markteintritt neuer Wettbewerber	Sachanlageschäden, z. B. infolge von Feuer
Zinsänderungsrisiken	Kostenstrukturrisiken
Adressausfallrisiken, insbesondere Ausfall von Kundenforderungen	Kalkulationsrisiken, insbesondere bei langfristigen Verträgen und im Projektgeschäft
Währungsrisiken, die laufende Transaktionen, Forderungen bzw. Verbindlichkeiten und/oder die Wettbewerbsposition betreffen	Risiken durch unzureichende Frühaufklärung (z. B. bzgl. technologischer Trends oder Aktivitäten der Wettbewerber)

Als wichtiges Hilfsmittel bei der Identifikation der wichtigsten Unternehmensrisiken kann die im Folgenden aufgeführte Checkliste dienen (vgl. Tab. 3.1). Allerdings können je nach Beschaffenheit des Unternehmens und seines Umfeldes auch noch weitere Risiken entscheidende Bedeutung besitzen, weshalb die hier genannten Punkte nicht als abschließend zu betrachten sind.

3.2.2 Ursachen-Wirkungsprinzip

Das Zusammenspiel von Ursache und Wirkung wird auch Kausalität genannt. In der Wissenschaft gehören diese beiden Begriffe stets zusammen. Die Kausalität wird als eine Folgerung verstanden. „Aus A folgt B“ oder aus „aus B könnte A resultieren“ beschreibt das Ursachen-Wirkungsprinzip. Eine Wirkung auf ein Unternehmen hat somit immer eine bestimmte Ursache und diese muss innerhalb des Risikomanagements genauer analysiert

und beurteilt werden. Oftmals wird fälschlicherweise die Korrelation mit der Kausalität gleichgesetzt, was jedoch falsch ist. Die Kausalität ist nicht gleichzusetzen mit der Korrelation. Eine Korrelation ist immer auf statistische Daten zurückzuführen, die Kausalität hingegen ist nicht auf diese Art von Daten zurückzuführen.

Im Kontext der Risikoanalyse dienen Ursache-Wirkungsmodelle der Veranschaulichung des unternehmerischen Risikoverständnisses. Risikofaktoren bezeichnen Einflussgrößen oder Ursachen, aus denen Risiken entstehen können. Die Risikofaktoren wirken auf die Risikoträger, die entweder Unternehmen selbst im Zuge der Selbsttragung (zum Beispiel als Selbstbehalt einer Versicherungspolice) oder nach einem Risikotransfer die Versicherungsgesellschaft betreffen. In einem Schadenfall bezeichnet der Risikofaktor die Schadenursache. In Abhängigkeit der Verwundbarkeit des jeweiligen Risikoträgers entstehen aus Risikofaktoren unterschiedliche Risikoereignisse. Ein vereinfachtes Modell ist in Abb. 3.1 dargestellt.

3.2.3 Analysemethoden

Die Risikoanalyse betrachtet die auf das Unternehmen einwirkenden identifizierten Risiken ganzheitlich und hinsichtlich ihrer Korrelation. Die Risiken werden nach ihrer jeweiligen Eintrittswahrscheinlichkeiten und quantitativen Auswirkungen bewertet. Verschiedene Analysemethoden helfen dabei eine fundierte Risikoanalyse durchzuführen und stellen sicher, dass auch alle Risiken miteinbezogen werden. Insbesondere sind die Kombinationseffekte der verschiedenen Risiken zu beachten. Denn die „schwerwiegendsten“ Schäden entstehen meist aus einer Kombination von verschiedenen Risiken und nicht aus einem Risiko allein heraus (vgl. Gleißner 2017, S. 99 f.). In der Praxis wird oft auf eine szenario-basierte Analyse, eine Ursachen-Wirkungsanalyse und auf Entscheidungsbäume zurückgegriffen. Diese Analysemethoden sollen in diesem Kapitel genauer dargestellt werden.

Die szenario-basierte Analyse nutzt Simulationsverfahren, um die Auswirkung verschiedener Risiken auf die unternehmerische Zukunft zu veranschaulichen. Die Szenarien

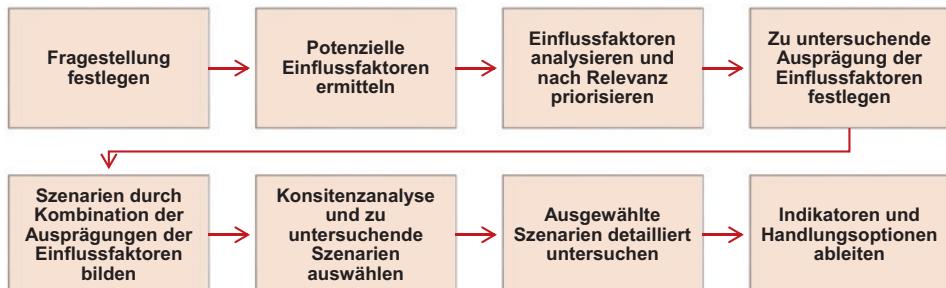


Abb. 3.1 Acht Schritte der Szenarioanalyse. (Quelle: eigene Darstellung in Anlehnung an Roemke 2019a)

fördern ein Vorausdenken. Es werden die Entwicklungen verschiedener Störungen analysiert und die daraus resultierenden Szenarien werden betrachtet. Die Entscheidungsträger werden durch die szenariobasierten Analyse auf zukünftige Ereignisse vorbereitet, nehmen die Wechselwirkung der verschiedenen Einflussfaktoren wahr und erhalten ein besseres Verständnis für kommende Entscheidungen und Ereignisse. Die verschiedenen Einflussgrößen und Charakteristiken müssen anhand der Szenarien dokumentiert werden (vgl. Siemes et al. 2014, S. 55). Herman Kahn und Anthony J. Wiener führten die Analysemethode 1967 in die Wirtschaftswissenschaften ein und definieren Szenarien als „*a hypothetical sequence of events constructed for the purpose of focussing attention on causal processes and decision points.*“ (Kahn et al. 1967, S. 6). Und weiter: „*They answer two kinds of questions: (1) Precisely how might some hypothetical situation come about, step by step? and (2) What alternatives exist, for each actor, at each step, for preventing, diverting, or facilitating the process.*“ (Kahn et al. 1967, S. 6). Ein mögliches Vorgehensmodell der Analyse besteht aus acht Schritten (vgl. Abb. 3.1).

Im ersten Schritt soll Klarheit erlangt werden, welche Themen untersucht werden sollen, und das Team soll ein gemeinsames Verständnis für das zu behandelnde Thema erhalten. Das gemeinsame Verständnis ist besonders wichtig, da alle Teammitglieder dieselbe Fragestellung bearbeiten und das Team in die gleiche Richtung arbeitet. Im nächsten Schritt müssen die Einflussfaktoren ermittelt werden. Diese können nach bekannten Strukturen, wie beispielsweise der PESTEL-Analyse, ermittelt werden. Wichtig ist bei der Ermittlung der Einflussfaktoren, dass diese wertfrei dargestellt werden. Die Faktoren sind somit nicht gut/schlecht oder stärker/schwächer, da ansonsten die Betrachtungsweise der Teammitglieder beeinflusst werden könnte.

Um die Analyse nicht zu komplex werden zu lassen müssen die ermittelten Einflussfaktoren im nächsten Schritt priorisiert werden. Hierbei sollten nicht mehr als zwanzig Faktoren am Ende der Priorisierung übrig bleiben. Werden die Faktoren nicht nach Priorität geordnet und aussortiert, besteht die Gefahr an der Komplexität der Analyse zu scheitern.

Im Anschluss werden durch Studien, Gruppendiskussionen und andere Hilfsmittel realistisch erscheinende Ausprägungen der Einflussfaktoren festgelegt. Falls keine Studien oder andere externe Quellen herangezogen werden können, kann sich auch auf die Intuition des Teams verlassen werden.

Im nächsten Schritt werden durch die Kombinationen der Einflussfaktoren in verschiedenen Ausprägungen mögliche Szenarien dargestellt. Es ist wichtig zu überprüfen ob die einzelnen Faktoren sich nicht gegenseitig widersprechen. In diesem Fall spricht man von konsistenten Szenarien.

Die Analyse kann anhand einer Konsistenzmatrix erfolgen oder durch eine paarweisen Analyse. In diesen Schritten werden auch inkonsistente Szenarien aussortiert.

Die entwickelten Szenarien werden in den letzten beiden Schritten hinsichtlich der Fragestellung untersucht, es werden Handlungsoptionen und deren Wirkungen erfasst. Anhand der gesammelten Informationen werden konkrete Handlungsempfehlungen entwickelt. Ebenso werden auch Frühindikatoren für den Eintritt verschiedener Szenarien

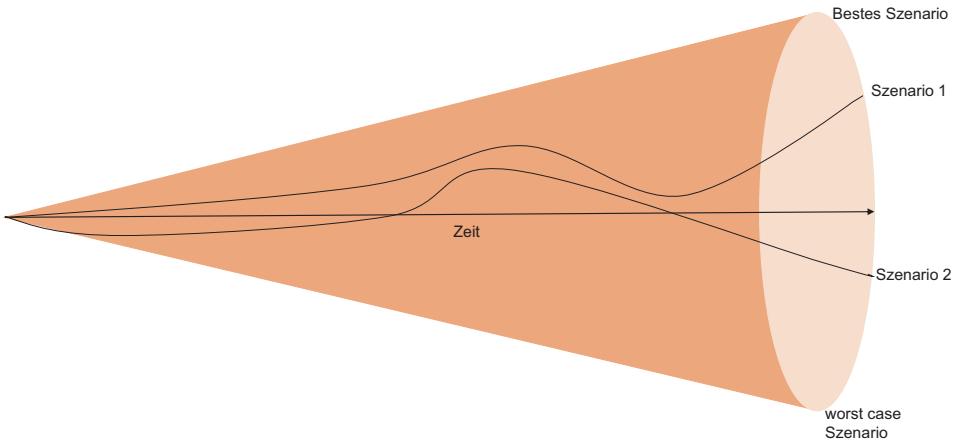


Abb. 3.2 Szenariobasierte Analyse

festgelegt. Diese Indikatoren sollen frühzeitig ein gewisses Szenario ankündigen und als Frühwarnsystem gelten (vgl. Abb. 3.2).

Die Szenarioanalyse kann einfach visualisiert werden. Der Anfangspunkt spiegelt den aktuellen IST-Zustand wider, der Trichter zeigt die zukünftigen Entwicklungen des Unternehmens auf. Diese können sowohl positive, als auch negative Auswirkungen haben. Der obere Rand des Trichters ist dabei das best-case- und der untere das worst-case-Szenario. Die möglichen Szenarien, die aus der Analyse resultieren liegen zwischen diesen beiden Punkten. Ebenso kann ein mögliches Zielszenario innerhalb dieses Kegels angesetzt werden (vgl. Romeike 2019a).

Eine weitere Analysemöglichkeit ist das Ursache-Wirkungs-Diagramm, welches auch oft Fischgrätdiagramm genannt wird. Dies ist auf die Optik des Diagrammes zurückzuführen. Die Gräten repräsentieren die Haupteinflussgrößen die das Problem auslösen, welches als Kopf des Diagrammes dargestellt ist. Als Haupteinflussgrößen werden oft die Punkte Management, Maschine, Material, Mensch, Methodik und Milieu genutzt. Diese sechs Einflussfaktoren werden als die „6 M“ bezeichnet und sollen das komplette Umfeld des Unternehmens widerspiegeln. Es werden interne und externe Ursachen analysiert. Das Ursachen-Wirkungs-Diagramm wird oft in Teamsitzungen erstellt, damit im Prozess alle Beteiligten miteinbezogen werden können. Die Haupteinflussgrößen können noch in Einzelursachen unterteilt werden. Die Einzelursachen können durch fünf warum-Fragen hinterfragt werden. Es wird fünfmal gefragt, da die erste Antwort oftmals nicht die gewünschte Antwort und somit die wahre Problemursache liefert. Wie auch bei der szenariobasierten Analyse kann das Ursachen-Wirkungs-Diagramm je nach Komplexität des Problems sehr umfangreich und unübersichtlich werden. Jedoch hilft das Diagramm dabei die Hauptursache eines Problems herauszuarbeiten und fokussiert sich dabei nicht nur auf eine oder zwei Ursachen, sonder auf ein ganzheitliches Unternehmensbild. Ein solches Diagramm

zu erstellen ist eine leicht anwendbare und erlernbare Methode um die Ursache eines Problems zu analysieren (vgl. Syska 2006, S. 64 f.).

Die dritte Analysemöglichkeit sind Entscheidungsbäume. Wie die beiden zuvor beschriebenen Methoden ist auch der Entscheidungsbaum einfach zu verstehen und leicht darzustellen. Die grafische Darstellung von komplexen Situationen hilft in diesem Fall dabei, diese verständlich darzustellen. Wie auch bei der Szenarioanalyse können die Szenarien dargestellt werden und sowohl der beste als auch der schlechteste Ausgang kann gezeigt werden. Die Entscheidungsbäume bilden unternehmerische Ereignisse ab. Entscheidungsknoten, Ereignisknoten und Konsequenzen bilden gemeinsam einen Entscheidungsbaum. Durch Linien werden die verschiedenen Punkte miteinander verbunden und stellen Entscheidungen und Ereignisse inklusive ihrer Eintrittswahrscheinlichkeiten dar. Ebenso müssen die Konsequenzen mit Geldeinheiten belegt werden. Aus den vorhandenen Eintrittswahrscheinlichkeiten und Geldwerten wird die Eintrittswahrscheinlichkeit als Produkt dieser Größen gebildet. Es können somit also die verschiedenen möglichen Strategien des Unternehmens bewertet werden. Unternehmen können mittels Entscheidungsbäumen komplexe Strukturen übersichtlich und monetär abbilden. Ebenso können verschiedene Risiken durch die Wahrscheinlichkeiten miteinander vernetzt werden und die Wechselwirkung der verschiedenen Risiken aufeinander kann mit in die jeweilige Strategie aufgenommen werden (vgl. Pastors 2008, S. 34 f.).

3.2.4 Wechselwirkung

Die Risiken nur zu erfassen und diese zu überwachen nutzt im Risikomanagementprozess wenig. Das Risikoinventar spiegelt lediglich die Einzelrisiken und deren Auswirkungen wider. Um risikogerechte Maßnahmen zu entwickeln und diese zu bewerten reichen eine reine Risikoanalyse und die Überwachung der Risiken nicht aus. Risikoorientierte Unternehmen können durch die Risikoaggregation existenzbedrohende Krisen frühzeitig erkennen und die getroffenen Handlungsoptionen bestmöglich einsetzen. Denn meistens nimmt die Kombinationen von Einzelrisiken ein bestandsbedrohendes Ausmaß an und führt zu Krisen oder sogar Insolvenz. Aus diesem Grund müssen die Kombinationseffekte der Risiken analysiert werden. Die Risikoaggregation soll den Gesamtumfang der Risiken darstellen. Zur Bestimmung müssen die Wechselwirkungen bzw. die Korrelationen der Einzelrisiken auf Ebene der Risikoarten, -kategorien und -bereiche ermittelt werden. Es werden mittels Korrelationsanalysen stochastische Zusammenhänge zwischen den verschiedenen Risikopositionen untersucht. Die Aggregation der Risikopositionen ist also stark durch die Korrelationen der Wahrscheinlichkeitsverteilungen geprägt. Können die Zusammenhänge mit „je-desto“ beschrieben werden, beispielsweise „je öfter die Maschinen ausfallen, desto geringer sind die möglichen Absatzmengen“, lassen sich Korrelationen einfacher bestimmen. Problematisch wird es bei ereignisorientierten Risiken, wie dem Ausfall eines Lieferanten oder einer Produktionsstätte. In diesem Fall können keine mathematisch korrekten Lösungen gegeben werden, aus diesem Grund werden durch Simu-

lationsverfahren Näherungslösungen bestimmt (vgl. Siemes et al. 2014, S. 49 f.). Unternehmerische Entscheidungen werden nach dem Gesamtrisikoumfang getätigt, da Eigenkapitalbedarfe oder Erträge an diesen gebunden sind. Um einen kompletten Prozess vorweisen zu können, müssen Unternehmen eine simulationsbasierte Risikoaggregation durchführen. Um einen guten Risikomanagementprozess durchzuführen, müssen die Risikoaggregationsverfahren Risiken durch beliebige Wahrscheinlichkeitsverteilungen erfassen, Verknüpfungen zwischen den Risiken erfassen, welche nicht additiv sind, und auf zukünftige Ratings und Unternehmensplanungen eingestellt sein. In der Literatur wird oftmals eine Normalverteilung herangezogen, um unternehmerische Risiken zu modellieren. Die Normalverteilung passt jedoch eher auf Finanz- und Markttrisiken, wohingegen unternehmerische Risiken durch eine linksschiefe Verteilung approximiert werden können, da diese Risiken selten in einer kurz- oder mittelfristigen Betrachtung katastrophale Verluste verursachen. Die Beurteilung der simulierten Verteilungen wird am besten mit einem Value-at-Risk-Model abgeschätzt (vgl. Gleißner 2017, S. 45 ff.).

Der Value-at-Risk (VaR) gibt den Maximalverlust eines Risikoportfolios in Geldeinheiten an, der in einem angegebenen Zeitabschnitt zu einem gegebenen Konfidenzniveau nicht überschritten wird. Das spezifische Konfidenzniveau wird als $1 - \alpha$ dargestellt und stellt die Wahrscheinlichkeit dar, mit der ein eintretender Schaden nicht überschritten wird. Also wird nur in $\alpha\%$ aller Fälle ein Verlustszenario, welches den VaR-Wert überschreitet, eintreffen. Durch das Risikomaß können Risikopotenziale bestimmt werden und durch eine einzige absolute Zahl können die unterschiedlichen Aggregationsstufen zusammengefasst werden. Es werden Wahrscheinlichkeitsverteilungen benötigt, in denen alle möglichen Szenarien widergespiegelt werden, um die Wertentwicklung des Risikoportfolios beurteilen zu können. In der Unternehmenspraxis geschieht dies meist mit Tabellenkalkulationsprogrammen oder Simulationssoftware. Die Wahrscheinlichkeitsverteilung für potenzielle Gewinne oder Verluste ergibt aus einer großen Anzahl der Differenzen der Werte eines Portfolios zu bestimmten Szenarien und des aktuellen Portfolios. Im Anschluss wird das Quantil, also der Wert der Verteilung, bestimmt, den das Portfolio mit einer bestimmten Wahrscheinlichkeit nicht unterschreitet.

Zur Ermittlung des VaR sind fünf Prämissen festzulegen. Es ist zu beachten, dass sich die Werte bei unterschiedlichen Prämissen im selben Risikoportfolio stark unterscheiden können. Aus diesem Grund ist es wichtig sich auch die Prämissen der VaR-Ermittlung genau zu überlegen und ggf. die Anpassung der verschiedenen Werte in Betracht zu ziehen.

1. Die Risikoposition beschreibt, welche Risiken einbezogen werden. Diese kann aus einem Einzelrisiko, einem Risikoportfolio, welches sich aus mehreren Einzelrisiken zusammensetzt, oder ein ganzer Unternehmensbereich, der aus vielen Risikoportfolios resultiert, bestehen.
2. Risikoparameter beeinflussen den Wert der Risikoposition maßgeblich und müssen aus diesem Grund auch zur Berechnung identifiziert werden. Die Parameter, so wie auch die Position, sind durch unternehmensindividuelle Faktoren geprägt. Diese Faktoren

sind beispielsweise Geschäftstätigkeit, Kapitalstruktur oder die Branche des Unternehmens.

3. Der Beobachtungszeitraum stößt in der Unternehmenspraxis oftmals auf eine gewisse Schwierigkeit. Denn die bestmögliche Länge kann unterschiedlich eingeschätzt werden. So kann ein kurzer Zeitraum den Vorteil haben, nur aktuelle Daten einzubeziehen, es kann aber auch zu einer Überschätzung des Risikos führen. Der Beobachtungszeitraum ist ein wichtiges Merkmal, da aus der Erfahrung der Vergangenheit die Aussagen über die Zukunft getroffen werden.
4. Die Haltedauer ist vor allem bei Aktien und Anleihen ein wichtiger Parameter. Sie bezeichnet den Zeitraum, zwischen dem die Risikoposition aufgelöst wird und der Risikoanalyse. Immobilien und Maschinen, die nicht leicht liquidierbar sind, müssen geschätzt werden. Leicht zu liquidierende Positionen bekommen hierbei eine kurze Haltedauer, schwer liquidierbare eine lange. Dies führt in der Berechnung zu ungenaueren Ergebnissen und kann zu unscharfen Werten führen.
5. Letztlich muss das Konfidenzniveau festgelegt werden. Das Konfidenzniveau hält hierbei die anfänglich beschriebenen Eigenschaften (vgl. Diederichs 2013, S. 156 ff.).

Um den VaR zu ermitteln, gibt es verschiedene Methoden, die sich in ihrer Vorgehensweise und in ihren Ergebnissen unterscheiden. Diese werden meist in parametrische- und nicht-parametrische Ansätze eingeteilt.

Nicht-parametrische Ermittlungen generieren ihre Parameter aus historischen Daten. Es werden keine Parameter der Verteilung aus theoretischen Verteilungen geschätzt, sondern aus den empirisch gefundenen Werten ermittelt. Die bekanntesten Simulationen sind die Monte-Carlo-Simulation und die Historische Simulation.

Die parametrische Ermittlung geht davon aus, dass die Parameter der Verteilung anhand einer bestimmbarer Verteilung geschätzt werden können. Es wird angenommen, dass eine analytisch bestimmbar Verteilung die Schäden der Risikopositionen darstellen kann (zum Beispiel Normalverteilung, Weibullverteilung oder Student-t-Verteilung). Der bekannteste Ansatz ist der auf der Portfoliotheorie nach Markowitz basierende Varianz-Kovarianz-Ansatz. Zu Beginn werden die einzelnen Varianzen der Risikopositionen des gesamten Portfolios ermittelt. In der Praxis wird oft nur auf eine ausgewählte Anzahl von Risikopositionen zurückgegriffen, da es bei zunehmender Anzahl der Risiken eine exponentielle Steigerung der benötigten Datenmengen gibt. Die Berechnung könnte in diesem Fall unmöglich oder sehr aufwendig werden. Im Anschluss daran bestimmt man die Varianz des kompletten Risikoportfolios unter Berücksichtigung der Verbundeffekte. Die Verbundeffekte werden durch die jeweiligen Kovarianzen dargestellt. Im letzten Schritt lässt sich die Standardabweichung des Portfolios bestimmen und hieraus schlussendlich der Var.

Historische Simulationen stützen sich auf Daten aus der Vergangenheit und verzichten somit völlig auf analytische Untersuchungen der Risiken. Es wird unterstellt, dass sich die Risikopositionen in der Zukunft genauso beeinflussen, wie sie es bereits in der Vergangenheit getan haben. Der große Vorteil von historischen Simulationen ist ihre Einfachheit. Es

werden keine so großen mathematischen Voraussetzungen benötigt, um diese Simulationen im Unternehmen zu implementieren, da kein spezielles stochastisches Modell unterstellt wird. Die Daten, welche zur Modellierung der Verteilung notwendig sind, können aus unternehmensinternen und externen Datenbanken genommen werden. Der Griff zu externen Daten ist gerade dann von Vorteil, wenn bestimmte Risikopositionen im Unternehmen selbst relativ selten auftreten, aber ein hohes Schadenausmaß haben können. Probleme treten auf, wenn die historischen Daten nicht repräsentativ genug sind und somit keine gute Aussage über zukünftige Schäden getroffen werden kann. Ebenso können für Risikopositionen, welche noch nie beobachtet worden sind, keine Ereignisse simuliert werden. An dieser Stelle ist zum Beispiel das Cyberrisiko aufzuführen, welches in den letzten Jahren stetig größer wird, es jedoch nicht genügend historische Daten gibt. Es können bestimmte Gewichtungsfaktoren eingebaut werden, um dieses Problem zu hemmen. Für Risikopositionen, die sich schnell ändern und neu sind, wie dem Cyberrisiko, sollten zusätzlich Szenarioanalysen durchgeführt werden. Das Risiko kann so ohne stochastische Modelle analysiert werden (vgl. Siemes et al. 2014, S. 51 ff.).

Die Berechnungsmethode mittels Monte-Carlo-Simulationen hat den größten Rechenaufwand und die größte Komplexität der verschiedenen Verfahren. Denn um eine geeignete Verteilung zu finden werden sehr viele Szenarien simuliert und diese dann letztendlich zu einer passenden Verteilungsfunktion zusammengestellt. Dennoch ist sie den anderen Methoden gegenüber, wegen der enormen Flexibilität, stark im Vorteil. Monte-Carlo-Simulationen basieren auf stochastischen Modifikationen der unterschiedlichen Modellparameter. Ebenso werden auch die Korrelationen zwischen den Risikopositionen mitberücksichtigt. Denn Monte-Carlo-Simulationen können unter Abhängigkeit vom Zufall mathematische Größen durch stochastische Simulationen näherungsweise bestimmen. Um die Parameter der Monte-Carlo-Simulation zu schätzen werden im ersten Schritt die historischen Zeitreihen genutzt. Da diese Simulationen mit Zufallsparametern arbeiten können beliebige Verteilungen, so wie fat tails und Extremszenarien sehr gut dargestellt werden. Ebenso ist es bei Monte-Carlo-Simulationen auch kein Problem eine große Menge an Risikopositionen unter verschiedenen Risikofaktoren zu bewerten (vgl. Romeike 2019b). In der Vergangenheit wurde diese Simulation sehr oft genutzt, da sie weniger stark von der Vergangenheit beeinflusst wird. Die Risiken werden als Schwankungsbreiten in der Gewinn- und Verlustrechnung bzw. der Bilanz mithilfe von Zufallsvariablen um den Planwert ausgedrückt. Dieses Planjahr wird daraufhin mehrere tausendmal durch unabhängige Simulationsläufe dargestellt. Aus den simulierten Werten ergibt sich dann die Wahrscheinlichkeitsverteilung. Die Parameter der Verteilung können dann aus diesen Werten bestimmt werden.

3.3 Risikobewertung

Die analysierten Risiken müssen im nächsten Schritt bewertet werden. Die klassische Risikobewertung teilt sich in qualitative und quantitative Bewertung auf. Im Anschluss an diese Bewertung müssen die Risiken unternehmensintern und extern berichtet werden, um ein einheitliches Bild über das Risikoportfolio des Unternehmens nach Innen und Außen widerzugeben. Das Reporting dient der Kommunikation des Risikoportfolios an die unternehmerischen Stakeholder sowie als Grundlage um den Risikobewältigungsmix vorzubereiten.

3.3.1 Qualitative und quantitative Risikobewertungen

Die Risikobewertung lässt sich in qualitative und quantitative Methoden einteilen. Oftmals wird in der Literatur auch von einer semi-quantitativen Methode gesprochen, diese ist als eine Mischform der vorherigen Methoden zu verstehen. Bei qualitativen Methoden werden keine eindeutig definierten Größen zugrunde gelegt, um die Risiken zu bewerten. Die Risikopositionen werden oft mit vernachlässigbar, selten, häufig oder katastrophal beschrieben. Qualitative Methoden bewerten das Risiko hingegen anhand eindeutig definierter Größen. Die Risiken werden meist anhand von statistischen Methoden beurteilt und dementsprechend in quantitativen Größen wiedergegeben. Diese sind in der Praxis oft das Schadenausmaß in Euro oder die Eintrittswahrscheinlichkeit in Prozent. Die Mischform der semi-quantitativen Methoden beschreibt das Risiko in Werteklassen. Diese sind oftmals in Eintrittswahrscheinlichkeiten oder Schadenhöhen „von – bis“ dargestellt.

Im Rahmen der qualitativen Bewertung wird für das Unternehmen eine spezifische Relevanzskala erstellt, die den Risikoappetit des Unternehmens widerspiegelt. Diese Relevanzskala besteht in der Regel aus fünf Relevanzklassen, in die ein potenzielles Risiko eingeordnet werden kann. Die Relevanzklassen unterscheiden sich dabei in der Höhe eines möglichen Schadens für das operative Betriebsergebnis. Die identifizierten Risiken

Tab. 3.2 Relevanzskala

Relevanzklasse	Bedeutung bzw. Ausprägung	Negative Wirkung auf den EBIT in %
1	Weniger bedeutende Risiken, die kaum spürbare Abweichungen vom EBIT verursachen	< 5 %
2	Mittlere Risiken, die spürbare Abweichungen vom EBIT bewirken	< 20 %
3	Bedeutende Risiken, die das EBIT stark beeinflussen oder sich auch langfristig auswirken	< 100 %
4	Schwerwiegende Risiken, die zu großen Abweichungen vom EBIT führen oder sich auch langfristig erheblich auswirken	≥ 100 %
5	Kritische Risiken, die den Fortbestand des Unternehmens gefährden können	> 400 %

werden somit auf Grundlage ihres möglichen Schadenpotenzials unterschiedlich wichtigen Relevanzklassen zugeordnet. Durch die Klassifizierung entsteht ein einfaches Ranking der identifizierten Risiken. Dies ermöglicht einen ersten Vergleich der Risikopotenziale und unterstützt bei der Priorisierung von Gegenmaßnahmen. Wichtig ist, dass die Relevanzskala erst nach der Risikoaggregation erstellt wird, andernfalls würden Aggregationsaspekte vernachlässigt und die Skala würde falsche Ergebnisse liefern, welche im Schadeneintrittsfall verheerende Folgen haben können. Unternehmen können sich durch eine Relevanzskala auf die wesentlichen Risiken des Unternehmens konzentrieren und eine zu komplexe und zu massive Untersuchung vermeiden. Ebenso können Informationen über die gesammelten Risikopositionen einfacher gesammelt und verbreitet werden. Es kann sich beispielsweise nur auf die drei „gefährlichsten“ Risikoklassen konzentriert und die anderen erst einmal außer Acht gelassen werden. In der nachfolgenden Tabelle wären das die Relevanzklassen 3 bis 5 (vgl. Tab. 3.2). Man könnte auch jedoch auch die zweite Relevanzklasse mit einbeziehen, um auch mittlere Risiken zu beachten.

Die Relevanzskala sollte auch herangezogen werden, wenn es um die Dokumentation, die Berichterstattung und die Überwachung von Risiken geht. Es sollte darauf geachtet werden, dass die jeweiligen Maßnahmen zur Relevanz der jeweiligen Risikoposition passen.

Die quantitative Bewertung hingegen ist deutlich umfangreicher und bildet die Grundlage für eine fundierte Risikoaggregation. Zusätzlich können in der Praxis auch zur Quantifizierung Szenario-Darstellungen gewählt werden. Die Risikoverantwortlichen schätzen die konkrete Wahrscheinlichkeit von Risikoszenarien ein. Es werden analog zur vorher beschriebenen Szenarioanalyse best- und worst-case-Szenarien festgelegt. Das Schadenausmaß wird über geeignete Verteilungsfunktionen dargestellt (zum Beispiel Normalverteilung oder Dreiecksverteilung). Zudem müssen Faktoren bestimmt werden, welche dazu führen, dass einer dieser Fälle eintritt und welche Risikopositionen einen maßgeblichen Einfluss auf das Ergebnis haben. Zusätzlich muss auch der geschätzte Effekt auf dieses Ereignis angegeben werden. Diese Einschätzungen sollten im besten Fall für die nächsten drei Jahre abgegeben werden. Auf dieser Grundlage können die möglichen Auswirkungen der Risikoszenarien auf die Unternehmensplanung simuliert und somit der Risikoumfang bestimmt werden.

Die Risikobewertung ermöglicht somit nicht nur eine Priorisierung der einzelnen Risiken, sondern dient als Grundlage zur Ermittlung des realistischen Gesamtschadenpotenzials für Unternehmen. Diese Bewertungsverfahren lassen sich ebenfalls auf das Chancenmanagement adaptieren.

3.3.2 Risikoreporting

Im folgenden Abschnitt wird das Risikoreporting genauer beschrieben. Um ein übersichtlicheres Risikoreporting im Unternehmen vorweisen zu können und die bewerteten Risiken besser darstellen zu können, wird in der Praxis auf verschiedene Darstellungsmöglich-

keiten zurückgegriffen. Das Reporting wird verwendet, um die Risiken zu visualisieren und eine bildliche Qualifizierung der Risikopositionen zu erstellen.

Die Risikomatrix oder auch Risk-Map genannt ist die häufigste genutzte Form der Visualisierung. Die Risikomatrix ist ein zweidimensionales Hilfsmittel, um die Risikopositionen quantitativ oder qualitativ darzulegen. Es müssen zwei Achsen gewählt werden, anhand welcher die Risiken gewertet werden können – typischerweise die Eintrittswahrscheinlichkeit und das Schadenausmaß. Die Risiken werden in der Risikomatrix eingetragen, somit erhält man eine Übersicht über die vorhandenen Risiken innerhalb des Unternehmens. Die Positionierung innerhalb der Matrix wird anhand der vorher bewerteten Ansätze vorgenommen. Hierbei sollte erneut der jeweilige Risikoverantwortliche mit einzogen werden, um eine klare Aussage über die jeweilige Position treffen zu können. Ebenso muss die Wechselwirkung der verschiedenen Risiken auch bei der Positionierung der Risiken beachtet werden. Bei der Anwendung der Risikomatrix wird implizit davon ausgegangen, dass ein Risiko überhaupt sinnvoll durch Schadenhöhe und Eintrittswahrscheinlichkeit beschrieben werden kann. Grundsätzlich ist zu beachten, dass Risiken mit gleichem Erwartungswert auf einer Hyperbel (nicht-linearer Zusammenhang) dargestellt sind und somit durch mehr als einen Quadranten der Matrix verlaufen können. Zudem besteht die Gefahr, dass gänzlich unterschiedliche Risiken in der Risikomatrix identisch abgebildet werden. Dies passiert, wenn das Risiko rein als potenzieller Höchstschaden („wort-case“) oft in Verbindung mit Expertenschätzungen interpretiert wird. Eine Sensitivitätsbetrachtung aus einem optimistischen (besten), einem pessimistischen (schlechtesten) und einem wahrscheinlichsten (normalen) Szenario kann dann dazu führen, dass zwei unterschiedliche Risiken in der Matrix an gleicher Stelle abgebildet werden.

Welche Kombination als kritisch angesehen wird und ab welchem Punkt eine unkritische Einstufung stattfindet, muss das jeweilige Unternehmen selbst einschätzen. Die Risikomatrix und die jeweiligen Folgen können somit zwischen verschiedenen Betrieben unterschiedlich aussehen. Ist der Risikoverantwortliche sehr risikotolerant, so wird der kritische Bereich kleiner ausfallen als bei risikoaversen Unternehmen. In Abb. 3.3 ist eine Risikomatrix dargestellt. Der obere Bereich rechts wird als kritisch angesehen. Der untere Bereich links spiegelt die Risiken dar, die vom Unternehmen als „sicherste“ wahrgenommen werden. Im mittleren Bereich finden sich die restlichen Risiken. Oftmals werden gerade diese Risiken unter- oder überschätzt.

Risiken können auch quantitativ iHinweise Verlag/Setzerei: n der Risk-Map eingeteilt werden. Dies ist in der Praxis oft der Fall, wenn ungenügende Informationen über die Risiken vorliegen. Die Eintrittswahrscheinlichkeit wird in diesem Fall oft in „selten“, „häufig“ und „sehr häufig“ eingeteilt und das Schadenausmaß in „gering“, „mittel“, „groß“ und „katastrophal“. In der Praxis können gerade Risiken wie Image- oder Reputationsschäden sehr schlecht mit tatsächlichen Werten belegt werden.

Vorbereitend für den Risikobewältigungsmix werden die Risiken in der Risikomatrix in verschiedene Klassen eingeteilt. Durch diese Klassifizierung kann genauer gesagt werden, was mit den jeweiligen Risiken passiert.

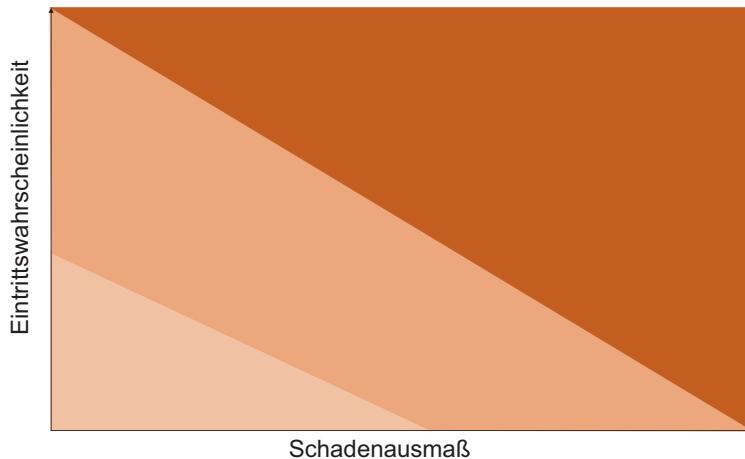


Abb. 3.3 Risikomatrix. (Quelle: eigene Darstellung)

3.4 Risikobewältigungsmix

Dieses Kapitel befasst sich mit dem wirtschaftlichen Umgang des Schadens und dessen Folgen oder kurz mit der Risikosteuerung. Es wird in erster Linie die Situation und die Möglichkeiten vor dem Eintritt und nach dem Eintritt des Ereignisses beurteilt und analysiert. Hierbei handelt es sich um einen Kreislauf, da der Zeitpunkt nach dem Eintritt auch gleichbedeutend mit dem Zeitpunkt vor dem nächsten Eintritt ist. Es muss somit ein ständiger Prozess neu durchlaufen und bewertet werden. In der Literatur wird dieser Zeitpunkt oftmals als Krisenmanagement bezeichnet. Eine Krise ist an dieser Stelle keine durchweg schlechte Situation, sondern eine Situation, in der maßgebende Entscheidungen für den restlichen Verlauf getroffen werden müssen.

Die Risikobewältigung zielt darauf ab, die Risikosituation gemäß der Risikophilosophie des Unternehmens zu beeinflussen. Eine optimale Bewältigungsstrategie trägt zur Sicherung des Unternehmenserfolges und zur Steigerung des Unternehmenswertes bei. Der Risikobewältigungsmix befasst sich mit dem Steuern von Unternehmensrisiken. Die verschiedenen Möglichkeiten im Umgang mit Risiken werden analog zum Ursachen-Wirkungsprinzip eingestuft. Hierbei gibt es ursachenbezogene Techniken und wirkungsbezogene Techniken. Bei ursachenbezogenen Ansätzen versucht man den Kern des Risikos zu analysieren und an dieser Stelle zu verbessern. Dies kann durch eine Risikominderung geschehen oder sogar durch eine Risikovermeidung. Im Gegensatz hierzu werden beim wirkungsbezogenen Ansatz darauf geachtet wie das Unternehmen mit der Auswirkung von eintretenden Risiken umgeht und wie die Auswirkung innerhalb des Unternehmens behandelt werden.

Es gibt verschiedene Bewältigungsmethoden, die von Unternehmen genutzt werden können.

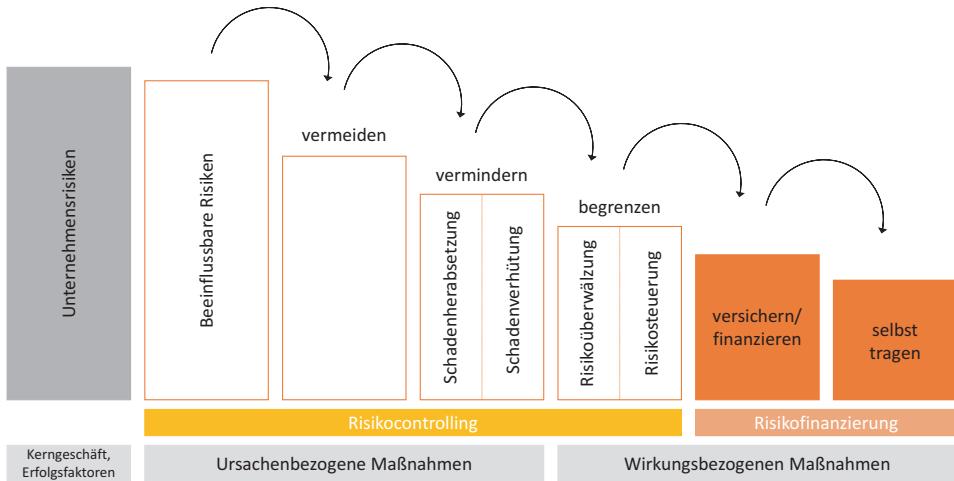


Abb. 3.4 Risikobewältigung. (Quelle: eigene Darstellung)

- Vermeiden: Es wird auf eine risikoreiche Aktivität verzichtet. Damit sollen Vermögensverluste vermieden werden, indem alle mit dem Risiko verbundenen Prozesse und Tätigkeiten eingestellt werden.
- Vermindern: Durch Maßnahmen kann einerseits die Reduktion der Eintrittswahrscheinlichkeit erreicht oder andererseits die Reduktion der realistischen Schadenshöhe bewirkt werden.
- Begrenzen: Bei der Risikoübertragung wird der Träger des Risikos gewechselt. Unternehmen können ihre Risiken dabei teilweise oder komplett auf andere Vertragspartner übertragen.
- Selbst tragen/versichern: Bei einer passiven Risikopolitik wird das Risiko akzeptiert und es werden Rücklagen für das Risiko gebildet. Eine weitere Möglichkeit bietet die Versicherung des vorhandenen Risikos.

Abb. 3.4 zeigt die schrittweise risikoreduzierende Risikobewältigung auf.

3.4.1 Kosten-Nutzenabwägung bei der Risikobewältigung

Maßnahmen zur Verminderung sind in der Regel mit Kosten verbunden und müssen dem reduzierten Schaden hypothetisch gegenübergestellt werden. Bei der Minimierung von Risiken ist stets eine Kosten-Nutzen-Analyse zu führen, um die gesparten Kosten nicht durch die eingesetzten Ressourcen aufzuzeihen. Die Kosten selbst können quantifizierbar und nicht-quantifizierbar (qualitativ-messbar) sein. Dies gilt auch für alle Kosten im Zusammenhang mit Risiken, die noch nicht/nie eintreten sind. Diese werden als „hypo-

thetische Vorteile“ bezeichnet. In der Realität messen Unternehmen dem „hypothetischen Nutzen“ aufgrund seiner Komplexität jedoch wenig oder gar keine Bedeutung bei.

Nicht-quantifizierbare Kosten hängen in hohem Maße von unternehmens-spezifischen Merkmalen, der Unternehmenskultur und/oder dem gesamten Unternehmen ab. Verschiedene Studien belegen, dass sich bei nicht quantifizierbaren Risikokosten ein Vielfaches der quantifizierbaren Kosten ergeben kann. Beispiele für nicht-quantifizierbare Kosten sind die Verschlechterung von Reputation oder Image sowie des Arbeitsklimas. Die quantifizierbaren Risikokosten lassen sich in direkte und indirekte Kosten aufteilen. Direkte Kosten sind sichtbar und offensichtlich, während indirekte Kosten verborgen und nicht sofort ersichtlich sind. Beispiele für quantifizierbare Risikokosten sind Gesundheitskosten, Produktivitäts-/Qualitätsverluste, Schäden an Gebäuden und Maschinen, höhere Produktionskosten oder auch höhere Versicherungsprämien. In einer Situation, in der es nicht zu eingetretenen Risiken kommt, führen die direkten Kosten zu direkten hypothetischen Vorteilen, während die indirekten Kosten zu indirekten hypothetischen Vorteilen führen. Die sich daraus ergebenden indirekten hypothetischen Vorteile umfassen zum Beispiel geringe Krankmeldungen/Arbeitsunfähigkeiten unter Mitarbeitern.

Obwohl hypothetische Vorteile eher theoretisch und konzeptionell zu sein scheinen, sind sie dennoch wichtig, um das Risikomanagement vollständig zu verstehen. Hypothetische Vorteile können vom Unternehmen durch Fragen festgestellt werden wie: „Wie viel kostet die Investition in eine Risikomanagement-Maßnahme oder einen Teil davon?“ Oder: „Was wäre der höhere Preis der Versicherungsprämie, wenn ein bestimmtes Risiko eintreten sollte?“. Hypothetische Vorteile aus nicht vorkommenden Schäden können in fünf Kategorien unterteilt werden:

1. Die erste Kategorie betrifft die Vermeidung des Ausfalls der Arbeitszeit von Personal und schließt Löhne sowie Gehälter ein. Im Risikofall bleibt das Unternehmen in der Regel auf diesen fixen Kosten sitzen.
2. Der „Nichtverlust“ (Erhalt) von kurzfristigen Vermögenswerten bildet die zweite Kategorie und kann zum Beispiel den Nichtverlust von Rohstoffen oder Fertigwaren umfassen.
3. Die dritte Kategorie umfasst langfristige Vermögenswerte wie den „Nichtverlust“ von Maschinen oder Gebäuden.
4. Verschiedene kurzfristige Vorteile aus vermiedenen Strafzahlungen oder Mehrkosten (zum Beispiel infolge von höheren Transportkosten im Schadenfall) bilden die vierte Kategorie.
5. Die fünfte Kategorie besteht aus dem Nichtverlust von Umsätzen und Erträgen (zum Beispiel aus einer Nicht-unterzeichnung von Verträgen oder die Vermeidung der Gewährung von Preisreduktionen).

Die sichtbaren oder direkten hypothetischen Vorteile (die sich aus der Vermeidung von Kosten aufgrund nicht auftretender Schäden ergeben) machen nur einen kleinen Teil der Faktoren aus, die für den hypothetischen Gesamtnutzen aufgrund nicht auftretender Schä-

den verantwortlich sind. Neben sichtbaren Vorteilen können auch unsichtbare Vorteile bestehen. Unsichtbare, nicht-quantifizierbare Vorteile können sich auf unterschiedliche Weise ergeben: Nichtverschlechterung des Images oder Vermeidung von Rechtsstreitigkeiten.

3.4.2 Ursachenbezogen

Ursachenbezogene Risikobewältigungstechniken sind aktive Maßnahmen innerhalb des Unternehmens. Diese Aktionen greifen aktiv in das Unternehmen ein und versuchen Risiken direkt zu vermeiden oder das Risiko zu vermindern. Innerhalb eines Unternehmens werden somit Risikostrukturen gestaltet. Es werden die Risikofolgen gemindert oder sogar vollständig bereinigt. Dies geschieht durch die Verringerung der Eintrittswahrscheinlichkeit und/oder des Schadenausmaßes des Risikos.

3.4.2.1 Vermeidung

Die Vermeidung von Risiken ist die naheliegendste Entscheidung im Umgang mit Risiken. Jedoch werden bei der Vermeidung nicht nur der Verlust ausgeschlossen, sondern auch die Chance, die mit dem jeweiligen Risiko einhergeht. Ebenso wird dem Unternehmen unter Umständen auch eine Verbesserung oder eine Erneuerung bestimmter Bereiche genommen, falls bestimmte Risikosituationen ausbleiben. Die Vermeidung von Risiken entsteht anhand der Eliminierung der Eintrittswahrscheinlichkeit bzw. des Schadenausmaßes. Bei der Vermeidung von Risiken werden bestimmte Risiken gar nicht erst eingegangen. Durch den Ausschluss dieser Risiken ändert sich die unternehmenseigene Risikoverteilung. Oftmals werden insbesondere Geschäftsbeziehungen oder Investitionen in bestimmte Länder, der Handel mit Derivaten/Options/Futures oder bestimmte Geschäftsbereiche vermieden. Unternehmen setzen auf altbewährte Techniken, um die mit neuen Techniken einhergehenden Risiken nicht eingehen zu müssen (vgl. Abb. 3.5).

3.4.2.2 Verminderung

Um Risiken zu vermindern, müssen diese besonders überwacht werden. Bei der Verminderung wird die Eintrittswahrscheinlichkeit und/oder das Schadenausmaß verringert (vgl. Gleißner 2017, S. 288). Die Minderung macht nur bei Risiken mit höheren Eintrittswahrscheinlichkeiten wirklich Sinn, da bei Risiken mit geringen Eintrittswahrscheinlichkeiten eine Reduzierung zu kostenintensiv im Vergleich zum Erfolg der Minimierung ist.

Eine der einfachsten Möglichkeiten Risiken zu mindern, ist die Schulung von Mitarbeitern. Das Trainieren der Belegschaft und die Sensibilisierung für gewisse Risiken verringert die Eintrittswahrscheinlichkeit von Risiken und kann sogar das Schadenausmaß beeinflussen. Die Schulung der Mitarbeiter sollte nicht nur auf die Einhaltung von Gesetzen und Vorschriften beschränkt sein, sondern muss auch Prozesse und die verbundenen Schritte beinhalten. Durch diese relativ kostengünstige Möglichkeit können Risiken effizient verringert werden. Ebenso müssen die Prozesse, welche die Mitarbeiter durchführen

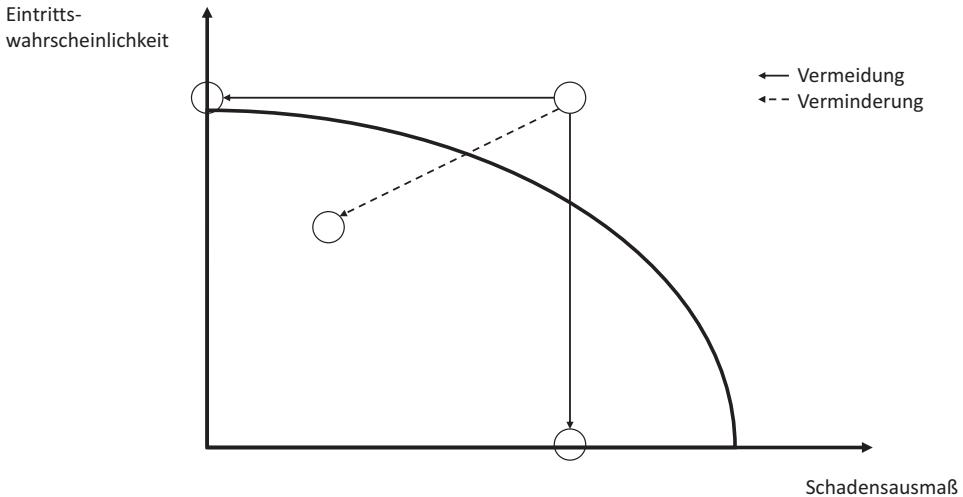


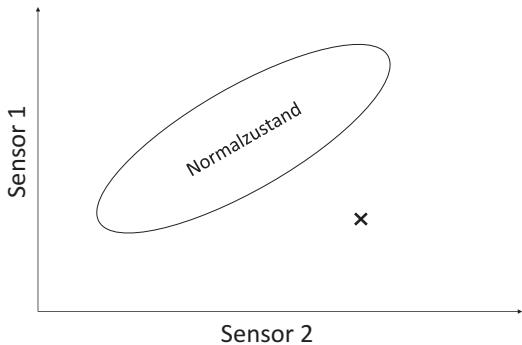
Abb. 3.5 Risikovermeidung und – minderung. (Quelle: eigene Darstellung)

sollen, klar strukturiert und sauber dokumentiert sein. Durch eine klare Prozessstruktur können Mitarbeiter die Anforderungen und Bedingungen des Risikomanagements einfacher verstehen. Dies führt zu präventiven Maßnahmen im Unternehmen. Ebenso können Risiken innerhalb des Unternehmens durch gezieltes und stetiges Monitoring verminder werden. Ereignisse, die in der Bewertungsphase festgelegt wurden, müssen dauerhaft beobachtet und angepasst werden. Bei Finanzrisiken kann das Monitoring beispielsweise durch Nachrichtensysteme wie Bloomberg oder Ähnliche einfach geschehen.

Technische Schäden innerhalb des Unternehmens können durch Sensoren beobachtet und somit gemindert werden. Hierfür muss anhand der vorliegenden historischen Daten ein „Normalzustand“ festgestellt werden und wie Abweichungen von diesem Zustand aussehen. Der Normalzustand muss anhand des Zusammenspiels von mehreren Sensoren oder Überwachungstools festgelegt werden.

In Abb. 3.6 ist das Monitoring anhand von zwei Sensoren vereinfacht dargestellt. Das Zusammenspiel der gemessenen Werte kann auf den Achsen eingetragen werden. Anhand der Werte kann ein Normalzustand festgelegt werden. Messwerte, die außerhalb des Normalzustandes liegen, sind durch das X dargestellt und können frühzeitig erkannt werden. In diesen Fällen muss der Mitarbeiter eingreifen, um das Risiko eines Verlustes zu minimieren und größeren Schaden zu verringern. Anhand von historischen Werten kann oftmals schon frühzeitig erkannt werden, wenn ein „Fehlzustand“ angesteuert wird. Es kann in diesen Fällen noch eingegriffen werden und somit eine Eskalation des Zustandes rechtzeitig unterbunden werden. In diesem Beispiel kann das Monitoring von technischen Maschinen nicht nur Risiken minimieren, sondern auch Kosten einsparen, da durch das ständige Monitoring gegebenenfalls Wartungskosten entfallen können (vgl. Campenhausen 2014, S. 24).

Abb. 3.6 Abweichung Normalzustand. (Quelle: eigene Darstellung)



Auch Stigmatisierungen des Unternehmens können und sollten beobachtet werden. Die Kommunikationsabteilung des Unternehmens kann die Nachrichten auf Nennungen verfolgen und diese dokumentieren. Die verschiedenen Nennungen des Unternehmensnamen müssen in negativ, neutral und positiv eingeordnet werden. Bei der Auswertung der dokumentierten Daten ist darauf zu achten, dass negative Nachrichten vermehrt auftreten werden, da es mehr negative Nachrichten in die Medien schaffen, als positive. Durch eine Beobachtung und Dokumentation dieser Daten kann zwar nicht das Eintreten direkt vermieden werden, es kann jedoch das Ausmaß direkt kontrolliert und eingedämmt werden. Wie in Abb. 3.6 dargestellt, wird das Risiko und die damit verbundene Wirkung nicht vollkommen eliminiert, da eine vollkommene Eliminierung dieses Risikos in der Praxis nicht möglich ist, es kann jedoch in einen akzeptablen Bereich gelenkt werden. Für die Überwachung dieses Risikos müssen in der Kommunikationsabteilung Spezialisten eingesetzt werden, die das Risiko dauerhaft dokumentieren. Diese Funktion kann auch von einem externen Dienstleister übernommen werden (vgl. Campenhausen 2014, S. 26 ff.).

Neben dem Monitoring von Risiken kann ein Risiko auch durch Diversifikation reduziert werden. Unter Risikodiversifikation versteht man das streuen von unabhängigen Risiken innerhalb des Unternehmens. Die Streuung kann regional, objektbezogen oder personenbezogen erfolgen. In der Praxis bedeutet das beispielsweise die Verteilung von Lagerorten. Es werden wichtige Produktionsmaterialien oder fertige Produkte an mehreren Orten gelagert, damit es beim Ausfall eines Standortes nicht zu einer kompletten Betriebsunterbrechung kommt. Die Risikodiversifizierung kann auch durch Outsourcing von bestimmten Unternehmensteilen geschehen. So können IT-Risiken durch dezentrale Rechnerstrukturen oder Outsourcing auf Cloudbasierte Systeme geschehen. Personenbezogene Risiken werden in der Praxis häufig durch Reiseregelungen reduziert. Durch reisen in separaten Flugzeugen oder Fahrzeugen können Kumulrisiken mit geringem Aufwand gemindert werden. Durch die Risikodiversifikation können im Unternehmen einfach Effizienzgewinne erzielt werden und das Risiko in einem akzeptablen Bereich verlagert werden (vgl. Romeike et al. 2013, S. 140 ff.).

3.4.3 Wirkungsbezogen

Wirkungsbezogene Maßnahmen innerhalb des Risikobewältigungsmixes konzentrieren sich weniger auf die Minderung der Eintrittswahrscheinlichkeit als auf die Reduzierung der Wirkung des jeweiligen Risikos auf das Unternehmen. Wirkungsbezogene Maßnahmen lassen sich grob in die Verlagerung der Wirkung und die Akzeptanz des Risikos und die damit zusammenhängende Wirkung einteilen. Wirkungsbezogene Ansätze können von aktiven Ansätzen bis hin zu passiven Maßnahmen reichen. Oftmals werden in der Praxis vor allem die Wirkungsbezogenen Maßnahmen mit der Steuerung von Risiken in Verbindung gebracht. Der folgende Abschnitt soll einen Überblick über die praxisrelevanten Methoden und Möglichkeiten zur Reduzierung der Auswirkung von eintretenden Risiken auf das Unternehmen darstellen.

3.4.3.1 Verlagerung

Das Risk Exposure eines Unternehmens kann durch das Verlagern eines Risikos auf ein externes Unternehmen reduziert werden. Bei der Verlagerung wird die Wirkung des Risikos auf die übernehmende Partei übertragen. Wird ein Risiko über einen Outsourcing-Prozess auf ein Subunternehmen umgelagert, entfällt zwar das eigentliche Risiko, es entstehen aber auch gleichzeitig neue Risiken. Verlagert ein Unternehmen beispielsweise die Teilproduktion auf ein anderes Unternehmen, so sind die mit der Produktion einhergehenden Risiken ausgelagert, es können jedoch neue Lieferantenrisiken entstehen. So kann es zu Lieferengpässen oder sogar dem kompletten Ausfall des Lieferanten kommen. Ebenso kann das Risiko auf Kunden und Partner verlagert werden. Bei dieser Art der Risikosteuerung muss die Verlagerung klar im Vertrag festgehalten werden und der übernehmenden Partei klar gemacht werden, damit es im Krisenfall nicht zu Streitigkeiten kommt.

Risiken die vom Unternehmen als zu groß angesehen werden können durch den Einkauf von Versicherung aus dem Unternehmen verlagert werden. Für welche Risiken diese Art der Verlagerung in Frage kommt, können Unternehmen aus der vorher erstellten Risikomatrix entnehmen und individuell entscheiden. In der Regel handelt es sich bei Risiken, für die Versicherungsschutz eingekauft wird, um Risiken, die eine geringere Eintrittswahrscheinlichkeit und ein relativ hohes Schadenausmaß haben. Bei Risiken mit hoher Eintrittswahrscheinlichkeit und hohem Schadenausmaß ist das versichern oftmals nur die zweite Wahl. Erstmals versucht man die Risiken durch vertragliche Ausschlüsse, wie vorher beschrieben, auf Kunden oder Partner auszulagern (vgl. Campenhausen 2014, S. 42 f.). Versicherungsunternehmen schätzen mittels versicherungsmathematischer Funktionen die Risiken ein und tarifiert diese. Versichern ist ein Ausgleich im Kollektiv über eine bestimmte Zeit. Der Versicherer sichert dem Versicherungsnehmer gegen die Zahlung einer Prämie zu, den Schaden, der durch ein abgesichertes Risiko entsteht, in einer gewissen Höhe im Eintrittsfall zu übernehmen. Man verlagert innerhalb des Unternehmens in diesen Fällen die Ungewisse Schadenzahlung im Eintrittsfall in fixe laufende Kosten. Im Normalfall versucht das Unternehmen die Prämie, also die fixen Kosten, so günstig wie möglich zu halten indem es die Risiken, welche es versichert, bereits selbst reduziert (vgl.

Campenhausen 2014, S. 54 f.). Das Versicherungsunternehmen versucht nur „gute“ Risiken zu zeichnen. Gute Risiken sind für das Versicherungsunternehmen Risiken, die eine geringe Eintrittswahrscheinlichkeit oder ein geringes Schadenausmaß haben. Schlechtere Risiken werden von der Versicherung höher bepreist als gute. Grundsätzlich lassen sich Versicherungen im traditionellen Sinne und ohne Personenversicherungen in vier Versicherungssparten einteilen. Sachversicherung sichert Einrichtungen und Gebäude gegen Feuer, Wasser etc. und die wirtschaftlichen Folgen ab. Schadenersatzzahlungen für Personen- oder Sachschäden an Dritte können mit einer Haftpflichtversicherung abgesichert werden. Technische Betriebseinrichtungen und die damit zusammenhängenden wirtschaftlichen Risiken bei Ausfall, sowie die Risiken, die bei Aufbau von technischen Bauwerken und Anlagen anfallen sind in technischen Versicherungen abgesichert. Die Transportversicherung sichert alle Gefahren ab, die während dem Transport von Waren oder Produkten entstehen.

Ein wichtiger Punkt bei der Verlagerung von Risiken mittels Versicherungen ist die Principal-Agent-Theorie. Die Principal-Agent-Theorie beschreibt das Verhalten von zwei Vertragspartnern, bei dem der Principal als Auftraggeber einen Agenten beauftragt. Die beiden Parteien haben in ihrer Beziehung jedoch unterschiedliche Interessen und wollen ihren eigenen Nutzen aus der Beziehung maximieren. Grundsätzlich herrscht zwischen beiden Parteien ein Wissensunterschied. Im Normalfall hat der Principal einen gewissen Wissensvorsprung dem Agent gegenüber. Für den Einkauf von Versicherung und somit für die Risikoverlagerung aus dem Unternehmen heraus hat der Versicherungsnehmer in den meisten Fällen einen Informationsvorteil. Diesen Informationsvorteil bepreist das Versicherungsunternehmen in der Regel auch in seiner Versicherung mit ein. Eine völlige Transparenz dem Versicherer gegenüber kann sich somit auch in der Prämie widerspiegeln und zu einer Kostenreduzierung führen. Es kann vorkommen, dass der Versicherungsnehmer besser ist als die Marktteilnehmer, diesen Vorteil dem Versicherungsunternehmen jedoch nicht zeigen kann. An dieser Stelle werden die unterschiedlichen Interessen gegenübergestellt.

Das Verlagern von Risiken mittels Versicherung wird in Industrieunternehmen in der Regel zentral organisiert. Die Organisation ist oftmals vom Risikomanagement abgekoppelt. Die Abteilung arbeitet aber sehr nah am Risikomanagement, um Risiken zielgerichtet beurteilen zu können. Im ersten Schritt prüft die Abteilung stets, ob Risiken selbst getragen werden können. Falls dies nicht der Fall ist, muss hierfür Versicherung eingekauft werden. In diesem Prozess muss stets eine Kosten-Nutzen-Analyse durchgeführt werden. In dieser Analyse muss ermittelt werden, ob sich die Versicherungslösung für das Unternehmen lohnt. Beim Einkauf von Versicherungen muss die Risikokultur des Unternehmens miteinbezogen werden. Es spielt der Preis pro Risiko eine große Rolle. So können die Preise zwischen zwei Unternehmen allein durch die Risikokultur stark voneinander unterscheiden. Ebenso muss die Risikotragfähigkeit des Unternehmens berücksichtigt werden. Alle Risiken selbst zu tragen, würde das Unternehmen ruinieren, somit muss auch das Einfluss finden. Auch die Gefahr, die mit versicherten Risiken einhergeht, muss beachtet werden, denn Unternehmen gehen Risiken, welche zu 100 Prozent versichert sind,

eher ein als andere Risiken. An dieser Stelle kann es zu Fehlallokationen führen (vgl. Campenhausen 2014, S. 59 ff.).

Zusätzlich zu den beschriebenen Maßnahmen können Unternehmen durch „alternativen Risikotransfer“ eine weitere versicherungsorientierte Lösung zur Verlagerung des Risikos ausüben.

3.4.3.2 Akzeptanz

Die Akzeptanz eines Risikos ist gleichzusetzen mit der Selbstversicherung eines Risikos. Das Unternehmen spart die Versicherungsprämie und muss im Schadenfall den Schaden selbst zahlen. Für kleine Risiken kann diese Möglichkeit herangezogen werden, wobei die Korrelationen der verschiedenen Risiken nicht außer Acht gelassen werden darf. Mittlere und große Risiken selbst zu tragen ist oftmals eine Entscheidung in Abhängigkeit von der Risikokultur. Vor allem bei diesen Risiken muss auf die Korrelation geachtet werden. Es ist oftmals eine Einzelfallentscheidung und keine grundlegende Entscheidung. Beispielsweise können Vollkaskoversicherungen von großen Unternehmen zu teuer sein, da in den meisten Fällen die Prämien die Schäden übersteigen (vgl. Campenhausen 2014, S. 63 f.).

Sichert ein Unternehmen Risiken nicht ab, entweder ganz bewusst oder unbewusst, so muss es im Schadenfall selbst für die Kosten aufkommen. Unbewusste Akzeptanz von Risiken kann aus einer fehlenden Identifizierung oder aus einer falschen Bewertung der Risiken stammen. Für diese Risiken kann keine Rückstellung oder Finanzierung erfolgen, da die Kosten des Risikos nicht bewertet wurden und somit keine Bewertung des zukünftigen Cash-Flows vorhanden ist. Falls diese unbewussten Risiken eintreten werden in diesem Jahr die Gewinne geschwächt. In schwachen Jahren kann dies sogar zu negativen Ergebnissen führen.

Alle Risiken, die bewusst selbstgetragen werden, sei es nach einer Minderung oder weil nur ein Teil verlagert wurde, müssen vorfinanziert werden. Dies geschieht über mehrere Rechnungsperioden. Zur Deckung der ungewissen zukünftigen Zahlungen kann der Gewinn herangezogen werden, dies führt wie oben beschrieben jedoch zu Umsatzeinbußen und gegebenenfalls sogar zu negativen Ergebnissen. Unternehmen müssen diese Risiken nach dem Prinzip einer ex-ante-Finanzierung aus Unternehmensmitteln abbilden. Aus diesem Grund können die Zahlungen auch aus stillen und offenen Reserven oder dem gezeichneten Kapital getragen werden. Der Mindestgewinn oder die offenen Reserven sollten erst als letzte Lösung herangezogen werden, um diese Zahlungen zu bedienen. Der einfachste Weg die Risiken selbst zu tragen ist die Bildung von Rückstellungen. Rückstellungen werden gebildet, um drohende Verluste oder ungewisse Verbindlichkeiten zu zahlen. Aus den Rückstellungen können die Verluste durch eintretende Risiken getragen werden und somit ein Verlust in Schadenjahren abgefangen werden. Unternehmen können Risiken auch über ein Funding abwickeln. Die höchste Form dieser Alternative ist die Bildung einer eigenen Captive. Captives (vgl. Romeike et al. 2013, S. 144 f.).

Die reine Selbsttragung ohne Rücklagen zu bilden und damit keine aktive Risikopolitik zu betreiben, dient dem Ausgleich von Chance und Risiko. Das Unternehmen setzt sich in

diesem Fall ganz bewusst gewissen Risiken aus, um die daraus resultierende Chance nutzen zu können (vgl. Romeike et al. 2013, S. 145).

3.5 Fazit

Die Analyse, Bewertung und Steuerung von Risiken innerhalb des Risikomanagementprozesses sind Hauptaufgabe des Risikomanagements und ein wichtiger Faktor zum Fortbestand des Unternehmens. Wesentlich bei der Durchführung dieser Punkte ist die ganzheitliche Betrachtung von Risiken innerhalb des Unternehmens. Risiken müssen im ersten Schritt einzeln analysiert und bewertet werden, jedoch dürfen bei diesen Schritten die Korrelationen zwischen den verschiedenen Risiken nicht vernachlässigt werden.

Die Analyse von Risiken innerhalb eines Unternehmens wird größtenteils anhand von mathematischen Grundsätzen durchgeführt und simuliert. Wichtig bei der Analyse und der einbezogenen Daten ist die Datenbasis, auf der die Simulation ansetzt. Historische Daten müssen stets auf den neusten Stand gebracht werden und auf Aktualität überprüft werden. Es ist beispielsweise nicht zielführend für Cyberrisiken die Daten der letzten 50 Jahre einzubeziehen, da diese sich nicht auf die aktuelle Situation beziehen lassen. Auch die Wechselwirkung der verschiedenen Risiken müssen bei der Einzelbetrachtung berücksichtigt werden.

Die Bewertung von Risiken ist sehr stark an die Risikokultur innerhalb des Unternehmens gekoppelt. Hierbei werden die Reporting-Tools bei gleichem Risikoportfolio zwischen verschiedenen Unternehmen sehr stark voneinander abweichen. Auch die zukünftige Abschätzung der Risiken ist bei der Bewertung ein wichtiger Punkt.

Beim Risikobewältigungsmix kommt es wie bei der Bewertung auf die Risikokultur des Unternehmens an. Das Unternehmen muss eine klare Linie in der Politik haben, welche Risiken selbstgetragen werden können und welche verlagert werden sollen. Die erste Maßnahme im Risikobewältigungsmix sollte aber immer die Minderung der Risiken sein. Die Minderung ist in den meisten Fällen die günstigste Methode. Selbst wenn Risiken verlagert werden, kann eine vorherige Minderung des Risikos die Versicherungsprämie senken. In vielen Fällen verlangt das Versicherungsunternehmen sogar eine Minimierung des Risikos in den Versicherungsbedingungen.

Literatur

- AGCS. (2020). Allianz-Risk-Barometer-2020. Zugegriffen am 21.02.2020.
- von Campenhausen, C. (2014). *Risikomanagement kompakt: Lektion 5: Risiken managen: Maßnahmen planen und umsetzen*. Eschborn: Management Circle.
- Diederichs, M. (2013). *Risikomanagement und Risikocontrolling* (3. Aufl.). München: Franz Vahlen (Finance Competence).
- Gleißner, W. (2017). *Grundlagen des Risikomanagements. Mit besseren Informationen zu fundierten Entscheidungen* (3. Aufl.). München: Franz Vahlen (Management competence).

- Gutenberg, E. (1962). *Unternehmensführung. Organisation und Entscheidungen*. Wiesbaden: Gabler (Die Wirtschaftswissenschaften, 4). <https://doi.org/10.1007/978-3-322-98981-9>.
- Hölscher, et al. (2002). *Herausforderung Risikomanagement. Identifikation, Bewertung und Steuerung industrieller Risiken* (1. Aufl.). Wiesbaden: Gabler.
- Kahn, H., et al. (1967). *The year 2000: A framework for speculation on the next thirty-three years*. Michigan: University of Michigan.
- Pastors, P. M. (2008). *Risiken des Unternehmens - vorbeugen und meistern*. Mering: Rainer Hampp.
- Rohlf, T. (2018). *Risikomanagement im Versicherungsunternehmen. Identifizierung, Bewertung und Steuerung* (2. Aufl.). Karlsruhe: VVW GmbH.
- Romeike, F. (2019a). Szenarioanalyse. (Hrsg.), v. RiskNET – The Risk Management Network. <https://www.risknet.de/wissen/rm-methoden/szenarioanalyse/>. Zugegriffen am 02.06.2019.
- Romeike, F. (2019b). Value at Risk. (Hrsg.), v. RiskNET – The Risk Management Network. <https://www.risknet.de/en/knowledge/rm-methoden/value-at-risk/>. Zugegriffen am 05.06.2019.
- Romeike, F., et al. (2013). *Erfolgsfaktor Risiko-Management 3.0. Methoden, Beispiele, Checklisten Praxishandbuch für Industrie und Handel* (3. Aufl.). Wiesbaden: Springer Fachmedien.
- Siemes et al. (2014): Risikomanagement kompakt: Lektion 3 Werkzeuge im Risikokreislauf: Identifikation, Bewertung, Aggregation. Zugegriffen am 01.06.2019.
- Skorna. (2013). Empfehlungen für die Ausgestaltung eines Präventionskonzepts in der Transportversicherung: Untersuchung von Transportschäden, Präventionsmaßnahmen und der Präventionsaffinität von Versicherungsnehmern. Zugegriffen am 27.05.2019.
- Syska, A. (2006). *Produktionsmanagement. Das A – Z wichtiger Methoden und Konzepte für die Produktion von heute* (1. Aufl.). Wiesbaden: Gabler.
- Wolke, T. (2009). *Risikomanagement* (2., vollst. überarb. u. erw. Aufl.). München: Oldenbourg. <http://www.oldenbourg-link.de/isbn/9783486587142>. Zugegriffen am 18.06.2019.

Dr. Alexander C. H. Skorna studierte am Karlsruher Institut für Technologie (KIT) Wirtschaftsinieurwesen und sammelte erste Praxiserfahrungen während seines Studiums in den USA, Singapur und Hong Kong. Im Anschluss erfolgte die Promotion an der Universität St.Gallen (HSG), Schweiz. Herr Dr. Skorna entwickelte dort Präventionslösungen sowie neue Vertriebsstrategien für die Versicherungswirtschaft und ist Autor zahlreicher wissenschaftlicher und praxisorientierter Fachpublikationen überwiegend in den Bereichen Supply Chain Risk Management, Prävention bzw. Schadenverhütung sowie Produkt- und Geschäftsmodellinnovation in der Versicherungswirtschaft. Nach einer Station als Risikoingenieur bei einem führenden deutschen Industriever sicherer verantwortet Herr Dr. Skorna seit 2014 den Bereich Business Development bei der Funk Gruppe, einem internationalen führenden Versicherungsmakler und Risikoberatungsunternehmen.

Philipp Nießen absolvierte im dualen System mit der Continentale Krankenversicherung a.G. und der Technischen Hochschule Köln den Bachelorstudiengang „Versicherungswesen“ mit den Schwerpunkten Risikomanagement, Bilanzierung von Versicherungsunternehmen und Versicherungsmathematik. Im Anschluss absolvierte er das Masterstudium Risk & Insurance an der TH Köln. Währenddessen arbeitete er als Business Analyst bei der Unternehmensberatung 67rockwell Consulting GmbH.



Effektive Risikokultur: Bedeutsam für Organisation, Kontrolle und Kommunikation von Risiken

4

Benedikt Hintze und Philipp Beuker

Zusammenfassung

Das vorliegende Kapitel soll einen Überblick über eine effektive Risikokultur im betrieblichen Risikomanagement geben. Dafür wird zunächst untersucht, was eine effektive Risikokultur beinhaltet und wie dies mit dem individuellen Risikobewusstsein der Mitarbeiter zusammenhängt. Daran angeschlossen wird das Risikomanagement als organisatorischer Rahmen für die Umsetzung der Risikokultur dargestellt. Hierbei werden insbesondere die Kontrolle und Kommunikation von Risiken vor dem Hintergrund einer effektiven Risikokultur betrachtet. Es stellt sich heraus, dass sich eine gelebte Risikokultur direkt auf das individuelle Risikobewusstsein der Mitarbeiter, eine nachhaltige Risikokontrolle und einen effektiven Informationsfluss auswirkt. Um die Risikokultur erfolgreich zu etablieren, sollten die verfolgten Ziele aus der Risikostrategie abgeleitet werden. Das Risikomanagementsystem bildet die Grundlage für eine risikoorientierte Entscheidungsfindung auf allen Ebenen einer Organisation. Eine effektive Risikokultur fördert das Risikomanagement nachhaltig und ist ein wichtiger Faktor für eine erfolgreiche Unternehmensführung.

B. Hintze (✉)

Georgsmarienhütte Holding GmbH, Georgsmarienhütte, Deutschland

E-Mail: Benedikt.Hintze@gmh-gruppe.de

P. Beuker

TH Köln, Institut für Versicherungswesen, Köln, Deutschland

E-Mail: philippbeukerweb@web.de

4.1 Risikokultur als Chance für zielführende Risikobewältigung

Unternehmerisches Handeln ist ohne Risiken nicht möglich, da die Zukunft und die Wirkung von Handlungen nicht vorhersehbar sind. Der Begriff und die Ziele einer nachhaltigen Risikokultur lassen sich auf das Unternehmen oder den einzelnen Betrieb grundsätzlich in ähnlicher Weise anwenden. In beiden Formen entstehen Risiken in unterschiedlicher Art und Weise, die erkannt und bewältigt werden müssen. Die Risiken eines Betriebs können sich aus den Produkten selbst sowie aus den einzelnen Produktionsfaktoren, wie zum Beispiel der menschlichen Arbeit, der Betriebsmittel oder der Werkstoffe, ergeben. Ziel des Konzepts einer Risikokultur ist ein systematisches und risikoangemessenes Verhalten unter allen Mitarbeitern auf allen Ebenen eines Betriebs. Kultur kommt vom lateinischen Wort „cultura“ und bedeutet so viel wie Anbau oder Pflege. Eine Risiko- und letztendlich Betriebskultur müssen angebaut und gepflegt werden. Dafür benötigt es ein einheitliches Verständnis der Risikokultur und des Risikobewusstseins ausgehend von der Geschäftsleitung bis zu einem angemessenen Verhalten aller verantwortlichen Mitarbeiter. Um eine effektive Risikokultur im Betrieb zu etablieren, muss man sich im Klaren darüber sein, was die Ziele einer Risikokultur sein sollten und was eine solche betriebsweite Kultur erfolgreich macht. Ein zentraler Aspekt der Risikokultur ist das Erreichen eines risikobewussten Handels bei den Mitarbeitern. Dafür muss man zunächst die Risikowahrnehmung der Mitarbeiter verstehen, um in der Folge ein möglichst einheitliches Bewusstsein zu schaffen. Sobald die Mitarbeiter für deren Verantwortung für die Risikoerfassung und die damit einhergehende Risikokommunikation sensibilisiert wurden, können klare Vorgaben für den Risikoumgang gesetzt werden.

4.1.1 Bedeutung einer effektiven Risikokultur

Jeder Betrieb geht Risiken ein, um seine Ziele zu erreichen. Die vorherrschende Risikokultur innerhalb des Betriebs kann das Management der Risiken vereinfachen oder erschweren. Sie beeinflusst wesentlich die Fähigkeit, strategische Entscheidungen unter Risiko zu treffen und Leistungsversprechen einzuhalten.

Die Risikokultur steht dafür, wie Risiken durch Geschäftsleitung und Mitarbeiter der Organisation betrachtet, beurteilt und behandelt werden. Darin eingeschlossen sind Aspekte wie Risikophilosophie und moralische Werte. Entscheidend ist jedoch, wie mit Risiken tatsächlich umgegangen wird. Dies kann losgelöst sein von formulierten Strategien, Richtlinien und Handbüchern. Die „gelebte Risikokultur“ kann als große Herausforderung im Risikomanagement angesehen werden. Sie entsteht aus dem wiederholten Verhalten aller Mitarbeiter. Diese Verhaltensweisen bestimmen sich durch unterschiedliche Werte, Überzeugungen und Einstellungen der Mitarbeiter (vgl. The Institute of Risk Management 2012).

► **Risikokultur:** Betrachtung, Beurteilung und Behandlung von Risiken im Unternehmen durch Vorstand, Aufsichtsrat und Mitarbeiter – mit eingeschlossen ist die Risikobereitschaft und moralische Werte.

Ausgangspunkt einer Risikokultur ist die Risikostrategie einer Organisation. Diese sollte sich an der ganzheitlichen Unternehmensvision, -strategie und -kultur des Betriebs orientieren und als wertschöpfender Prozess verstanden werden. Die Risikostrategie zielt darauf ab, welche Risiken das Unternehmen eingehen möchte und welche nicht. Zudem berücksichtigt sie den Risikoappetit und die Risikotragkraft. Damit die Gesamtheit der vom Betrieb eingegangenen Risiken nicht die Risikotragkraft übersteigt, muss ein betriebsweites Risikobewusstsein bzw. eine einheitliche Risikokultur entwickelt und aufrechterhalten werden (vgl. Diederichs 2018, S. 12). Innerhalb der Risikostrategie muss zudem erfasst sein, mit welchem Zeithorizont auf die Risiken geblickt wird. Die Ziele, die ein Betrieb mit der Risikostrategie verfolgt, leiten sich aus der allgemeinen Unternehmensstrategie ab. Sofern ein Unternehmen aus unterschiedlichen Geschäftssegmenten bzw. „Business Units“ besteht, kann es mehrere Risikostrategien geben.

► **Risikoappetit:** Bereitschaft eines Unternehmens oder einer Person, Risiken einzugehen. Kann Auskunft darüber geben, welchen Risikoumfang/-arten man bereit ist einzugehen, um seine Ziele zu erreichen.

Risikostrategie: Die Risikostrategie speist sich aus der Unternehmensstrategie. Mit Blick auf die Risiken bildet die Risikostrategie das Pendant zu den Chancen, die das Unternehmen ergreift. Die Risikostrategie regelt und ermöglicht den Umgang mit vorhandenen Risiken.

Risikotragkraft: Beschreibt das Risikodeckungspotenzial bzw. die Risikotragfähigkeit. Die wesentlichen Risiken eines Unternehmens sollten durch die Liquiditätsreserven abgedeckt sein, um die Ruinwahrscheinlichkeit möglichst niedrig zu halten. Die Risikotragkraft sollte immer größer als der Risikoappetit sein.

Das Ziel einer Risikokultur sollte sein, bei den zuständigen Mitarbeitern ein Bewusstsein über die Tragweite des eigenen Handelns in Bezug auf die Ziele des Betriebs zu entwickeln. Eine effektive Risikokultur ist somit jene, in der die Mitarbeiter auf informierter Weise die richtigen Risiken eingehen. Dafür benötigt es einen Rahmen, der eine entsprechende Informationsbeschaffung und Belohnung von sorgfältig vorbereiteten Entscheidungen ermöglicht. Das Risikomanagementsystem kann als ein solches Rahmenwerk angesehen werden (vgl. The Institute of Risk Management 2012). Es schafft die Grundlage für den einheitlichen Umgang mit Risiken auf allen Ebenen des Unternehmens. Neben den Schritten im Risikomanagement werden auch Zuständigkeiten und Verantwortlichkeiten festgelegt.

Im Rahmen der Risikokultur sollte eine Philosophie verfolgt werden, in der Risiken kommuniziert werden und nicht nach Schuldigen gesucht wird. Es sollte selbstverständlich sein, dass die Kenntnisse über betriebliche Risikosituationen möglichst ungefiltert ihren Weg zu den Vorgesetzten finden. Das benötigt einen lösungsorientierten Umgang mit Fehlern. Sollte in den betrieblichen Abläufen etwas schiefgehen, kann aus dem Fehler gelernt werden. Hierbei ist zu beachten, dass eine solche Fehlerkultur nicht in jedem Betrieb toleriert werden kann. Dies gilt insbesondere auf Gebieten mit Personenschaden- bzw. Großschadenpotenzials, beispielsweise in Luft- und Raumfahrt oder in einem Kernkraft-

werk. In solchen Betrieben muss die Risikokultur sehr streng und präventiv in Form einer Null-Fehler-Konzeption strukturiert sein, um irreparable Folgen zu vermeiden.

Vier Indikatoren bestimmen eine angemessene betriebliche Risikokultur. Es beginnt bei der obersten Führungsebene, dem sogenannten „**Tone from the Top**“ (vgl. Diederichs 2018, S. 15). Für eine Organisation ist es wichtig, eine einheitliche Risikokultur nachhaltig zu etablieren. Die Mitarbeiter in der Organisation sollten für den richtigen Umgang mit Risiken sensibilisiert werden. Das Risikobewusstsein der Mitarbeiter wird am besten durch gelebtes Vorbild der Führungskräfte gefördert. Die Geschäftsführung sollte zunächst Rahmenbedingungen zum Risikoumgang festlegen, beispielsweise in Form eines definierten Wertesystems und Risikoleitlinien. Dadurch ergibt sich für die Mitarbeiter ein Handlungsspielraum für Entscheidungen, damit die Risikotragkraft nicht überschritten wird. Das Management muss derartige Grundsätze in Abhängigkeit von dem Risikoappetit formulieren und diese durch Befugnisse in der Organisation konkretisieren. Mit einem definierten Wertesystem wird erreicht, dass sich die Mitarbeiter darüber bewusst werden, welche Risiken mit welchem Ausmaß bei ihren Entscheidungen hervorgerufen werden können (vgl. Diederichs 2018, S. 14). Es stellt damit die Grundlage für das Verhalten der Mitarbeiter dar. Es muss erfolgreich im Betrieb kommuniziert, beim Eingehen von Risiken beachtet und mit dem Risikomanagement und den internen Kontrollen verzahnt werden. Die Mitarbeiter sollten die Vorgaben und Leitlinien der Organisation zum Risikoumgang nachvollziehen und in der täglichen Arbeit umsetzen können. Sofern das Risikoverständnis der Mitarbeiter mit den Richtlinien zum Risikoumgang der Geschäftsführung übereinstimmt, kann von einer effektiven Risikokultur gesprochen werden.

► **Risikoverständnis:** Sichtweise auf ein Risiko vor dem Hintergrund der Risikobereitschaft, des Risikobewusstseins und der vorliegenden Informationen zu einem bestimmten Risiko. Es kann sich aus einem individuellen Risikoverständnis ein gemeinsames Risikoverständnis entwickeln.

Riskoumgang: Beschreibt die tatsächliche Handhabung mit einer Risikosituation. Die Handlungsaktivitäten im Riskoumgang ergeben sich aus dem Risikoverständnis.

Die **Charakteristika der Risikokultur** können in den Unternehmensbereichen voneinander abweichen. Die Risikokultur in der Forschung & Entwicklung ist von Ausprobieren und Scheitern gekennzeichnet. In der Buchhaltung herrscht hingegen ein hoher Grad an Genauigkeit. Von der Geschäftsleitung muss ein eindeutiger Standpunkt hinsichtlich des Risikoumgangs in den einzelnen Unternehmensbereichen kommuniziert werden. Dies beinhaltet auch den Umgang mit moralischen Grundsätzen sowie der Berücksichtigung weiterer Interessensvertreter innerhalb der Entscheidungsfindung. Eine den Zielen entsprechende Risikokultur kann jedoch nur erreicht werden, wenn das Management die Leitlinien ernst meint und auch sichtbar dauerhaft vorlebt. Denn reine Lippenbekenntnisse werden von der Belegschaft schnell enttarnt.

Ein weiterer Indikator stellt die **Verantwortlichkeiten der Mitarbeiter** dar (vgl. Diederichs 2018, S. 16). Die leitenden Angestellten sind das Bindeglied zwischen der Ge-

schäftsleitung und den einzelnen Geschäftsbereichen. Sie haben die Aufgabe, das Wertesystem und die Risikostrategie in die Unternehmensbereiche zu kommunizieren. Dabei müssen sie übergeordnete Risikoleitlinien des Betriebs beachten, die sich vorwiegend auf die allgemeine Aufbau- und Ablauforganisation im Risikomanagement beziehen. Die einzelnen Mitarbeiter stehen vor allem in der Verantwortung, ihre Tätigkeiten am Wertesystem, am definierten Risikoappetit und an bestehenden Risikolimits auszurichten.

► **Risikolimits:** Wesentliche Risiken werden begrenzt, beispielsweise im Betrag, zeitlich oder räumlich. Damit wird sichergestellt, dass eine festgelegte Verlusthöhe nicht überschritten wird.

Sie müssen sich über die Konsequenzen bewusst sein, die drohen, falls sie die von ihnen erwarteten Verhaltensweisen nicht erfüllen. Für den Fall, dass Mitarbeiter unangemessen hohe oder unerwünschte Risiken bzw. nicht tolerierte Geschäftsaktivitäten eingehen, sollten klare Konsequenzen definiert werden. Die Umsetzung einer wirksamen Risikokultur bedeutet daher auch Strafen gegenüber denjenigen Mitarbeitern durchzusetzen, die dem allgemeinen Wertesystem keine Beachtung schenken. In einem Betrieb mit unklarer Risikokultur können unbeabsichtigte Aktivitäten aus Versehen zugelassen sein, die den vorgegebenen Richtlinien widersprechen oder außerhalb der Vorgaben liegen. Dann bleibt es nicht bei dem Fehlverhalten des einzelnen Mitarbeiters. Es kommt auch dazu, dass andere Mitarbeiter oder ganze Bereiche die unpassende Entscheidungsfindung ignorieren, dulden oder nicht bemerken. Das kann die Erreichung strategischer, taktischer und operativer Ziele behindern. Im schlimmsten Fall führt dies zu ernsthaften Reputationsbeeinträchtigungen und finanziellen Schäden (vgl. The Institute of Risk Management 2012).

Daneben gilt es, eine **offene Kommunikation und kritischen Dialog** zwischen den verschiedenen Geschäftsbereichen und -abteilungen zu fördern. Damit wird die Beachtung der Risikokultur sichergestellt, um in der Folge Interdependenzen von Risiken zu erkennen. Eine Betriebsunterbrechung mag als Produktionsrisiko eingestuft werden, wirkt sich jedoch mannigfaltig aus. Es kann auch zu einem Umsatzausfall (Vertriebsrisiko) und einem Liquiditätsengpass (Finanzrisiko) führen, für den sich üblicherweise andere Unternehmensbereiche verantwortlich fühlen. Unterliegen Bereiche einer Organisation der Schweigepflicht gegenüber anderen Bereichen, ist nur ein eingeschränkter Dialog möglich (vgl. The Institute of Risk Management 2012).

Jeder Mitarbeiter sortiert, kategorisiert und filtert zwar unbewusst Informationen, dennoch kann mit der Risikokultur ein erheblicher Steuerungsimpuls gesetzt werden. Es ist zwar nicht möglich, absolute Klarheit bzw. Sicherheit über eine Risikosituation zu haben, jedoch sollte der Mitarbeiter Risiken bestmöglich einschätzen und eingehen können. Risiken bleiben durch mangelhafte Informationen unerkannt, wodurch die Ziele des Risikomanagements, nämlich die Sicherung des Unternehmensbestandes und die Sicherung des zukünftigen Erfolgs, bedroht werden.

Das Verständnis von alternativen Meinungen, konstruktiven Anregungen und offener Kritik ist förderlich für ein gemeinsames Risikoverständnis. Die Mitarbeiter sollten keine Angst davor haben, gegenüber ihren Vorgesetzten Bedenken über fragwürdige, unmoralische

sche oder illegale Praktiken zu äußern. Da diese Grundhaltung in der Betriebspraxis jedoch oft schwierig ist, sollten Instrument wie das Whistleblowing zum Einsatz kommen.

Für die Umsetzung der Risikokultur müssen auch **angemessenen Anreizstrukturen** geschaffen werden. Ein zentraler Aspekt für eine angemessene Risikokultur ist die Einbindung der Mitarbeiter in das Wertesystem und den Verhaltenskodex. Beispielsweise können Mitarbeiter, die potenziell risikorelevante Themen erkannt und wirksam kommuniziert haben, im Rahmen des Entlohnungssystems prämiert werden. Mit diesem Incentiven kann das Eigeninteresse des Mitarbeiters dem Unternehmensinteresse angeglichen werden, damit dieser nachhaltig im Rahmen der vorgegebenen Risikotoleranz agiert. Diese sogenannten „Incentives“ bzw. materielle und immaterielle Anreize garantieren jedoch kein moralisch und ökonomisch korrektes Verhalten.

Zusammenfassend kann man zwei ausschlaggebende Aspekte für die erfolgreiche Umsetzung einer einheitlichen Risikokultur erkennen. Zum einen die Sensibilisierung jedes einzelnen Mitarbeiters für die Risiken der Organisation und zum anderen die Schaffung eines Rahmens mit Richtlinien und Berichtswegen im Risikoumgang. Dies gelingt durch ein definiertes Wertesystem und Risikoleitlinien, die von dem Management dauerhaft vorgelebt werden.

4.1.2 Enges Zusammenspiel zwischen Risikokultur und Risikobewusstsein

Die Etablierung einer Risikokultur wird von dem Risikoverständnis der Mitarbeiter beeinflusst. Zur Umsetzung der Risikostrategie benötigt es eine effektive Risikokultur, mit dem Ziel ein unternehmensweites Risikobewusstsein zu schaffen. Dafür sollte das individuelle Risikoverständnis der Mitarbeiter an das definierte Wertesystem und den Risikoleitlinien angeglichen werden, um einen adäquaten Risikoumgang in den Geschäftsbereichen zu ermöglichen. Das subjektive Risikoverständnis einer Person setzt sich aus dem Risikobewusstsein und der Risikowahrnehmung zusammen.

► **Risikobewusstsein:** Stellt die Sensibilisierung eines Mitarbeiters für die Unternehmensrisiken dar. Basis für die Risikobewältigung.

Risikowahrnehmung: Beschreibt die individuelle Einschätzung eines Risikos. Mitarbeiter können verschiedene Auffassungen zum gleichen Risiko haben.

Risikobereitschaft: Individuelle Bereitschaft ein Risiko einzugehen, abhängig von der subjektiven Bewertung des Risikos.

Riskoverhalten: Erklärt das Verhalten in einer bestimmten Risikosituation, die durch mehrere Handlungsalternativen gekennzeichnet ist. Steht in einem engen Verhältnis zur individuellen Risikobereitschaft des Entscheidungsträgers und der Risikokultur des Unternehmens.

Das Risikobewusstsein beschreibt, in welchem Umfang Mitarbeiter in einer Gefahrensituation sich dessen bewusst sind. Es erklärt, inwieweit Mitarbeiter sich auch über den

vollen Umfang ihres Risikos im Klaren sind. Die Mitarbeiter sollten ein Risikobewusstsein aufbauen, mit der jede Risikolage eingeordnet und unabhängig bewertet werden kann. Wesentliche Risiken sollten umfangreich analysiert werden, um dann auf Grundlage hochwertiger Informationen eine risikobewusste Entscheidung zu treffen.

Das Risikobewusstsein einer Person ist stark davon abhängig, ob diese das Risiko überhaupt wahrnimmt. Die Risikowahrnehmung wird von Wissen, Emotionen und Trends beeinflusst und verdichtet sich zu einem Gesamtbild (vgl. Hirschmann 2015). Jeder Mitarbeiter kommt daher mit einer individuellen Risikowahrnehmung in ein Unternehmen. Was eine Person als Risiko wahrnimmt, muss für eine andere Person kein Risiko sein. Die Risikowahrnehmung wird darüber hinaus von Lebenserfahrungen, kulturellen Hintergründen und moralischen Werten beeinflusst, die möglicherweise im Widerspruch zu den vorgegebenen Richtlinien stehen.

Es sollten allerdings nicht ausschließlich Mitarbeiter eingestellt werden, die von vornherein bereits vollständig mit der Risikokultur des Betriebs übereinstimmen. Für ein langfristig risikoangemessenes Handeln sollte man in einem Betrieb versuchen, eine passende Mischung bei den Mitarbeitern zu finden. Diese Diversität durch vielfältige Risikotypen kann dem Unternehmen dabei helfen, neuen Situationen und Geschäfte erfolgreich einzugehen oder abzulehnen. Abhängig von der Situation braucht es einerseits Unternehmergeister, andererseits auch Kritiker. Das Ziel ist es, die richtigen Risikotypen für die richtigen Bereiche einzusetzen. Dies ist jedoch nicht immer möglich bzw. die Risikokultur kann sich in einem Betrieb über einen Zeitraum geändert haben. Deshalb sollte man das Risikobewusstsein seiner Mitarbeiter in den jeweiligen Bereichen möglichst regelmäßig einschätzen, auch vor Einstellung neuer Mitarbeiter.

► **Risikotypen:** Beschreibt die Risikobereitschaft einer Person in einer bestimmten Risikosituation, beispielsweise in den Ausprägungen risikoscheu und risikofreudig. Je nach Geschäftssegment sind unterschiedliche Risikotypen wünschenswert.

Die Risikowahrnehmung beruht auf Hypothesen, wodurch zu den gleichen Risiken unterschiedliche Meinungen, Vermutungen und Theorien aufgestellt werden (vgl. Hirschmann 2015). Es gibt objektivierbare Faktoren der Risikowahrnehmung, wie die Prognose der Eintrittswahrscheinlichkeit. Diese werden jedoch **subjektiv vom Individuum** hergeleitet. Die objektiven Faktoren lassen sich in der „echten“ Betriebsumwelt nicht immer einheitlich quantifizieren. Die Ermittlung einer Wahrscheinlichkeit wird dadurch schwierig bis unmöglich, jedoch nicht überflüssig. Die subjektive Risikoeinschätzung ermöglicht erst eine sorgfältige Begründung und Bewertung des Risikos.

Aus der Wahrnehmung und dem Bewusstsein über ein Risiko, folgt die Risikobereitschaft bzw. das **konkrete Risikoverhalten**. Die Risikobereitschaft variiert bei unternehmerischen Entscheidungen und bezieht sich auf den Umgang mit einem Risiko. Die Verhaltensforschung will die Risikobereitschaft von Probanden ermitteln mittels singulärer Laborexperimente und indem sie diese vermeintlich rational herausfordert. Im Ergebnis, so der Anspruch, können Personen eingeteilt werden in risikoscheue, risikoneutrale und

risikofreudige. Bei Risikoscheu, oftmals auch Risikoaversion tituliert, sei man einer Risikosituation grundsätzlich abgeneigt. Man wähle stets die Alternative mit geringerem oder gar keinem Risiko. Die Risikofreude beschreibt, dass positive Abweichungspotenziale vom Erwartungswert eines Risikos höher gewichtet werden als die Negativen. Bei Risiko-neutralität hingegen sei die Person bei der Entscheidung indifferent. Derart globale Einteilungen von Individuen werden inzwischen kritisch erachtet. Eine grundlegende Risikoaversion gibt es nicht. Sie ist nicht messbar. Jede Person agiert in ihrem ganz persönlichen Risikouniversum, das alle Risiken aufsummiert. Und je nach Situation drückt sich das im Risikoverhalten anders aus (vgl. Taleb 2018, S. 330 ff.). Zudem müsste man von einer Chancenaversion sprechen, wenn die Chance als die andere Blickrichtung auf ein Risiko verstanden wird. Von daher wird im Folgenden davon ausgegangen, dass es wichtiger für ein Unternehmen ist, überhaupt ein Risikobewusstsein bei den Mitarbeitern zu schaffen.

Jemand, der in der Vergangenheit risikoscheu gehandelt hat, kann in Zukunft durchaus bereit sein, höhere Risiken einzugehen. Zudem kann ein risikoscheues Verhalten auch negative Auswirkungen zur Folge haben. Ausschlaggebend ist hierbei die **Qualität der Entscheidungsfindung**. Denn dadurch erhöht sich die Wahrscheinlichkeit eines positiven Ergebnisses. Man kann auch eine überlegte Entscheidung getroffen haben, die sich dennoch später als nachteilig herausstellt. Das Ergebnis einer Handlung kann von Zufall beeinflusst werden. Daher sollte eine Entscheidung unter Risiko nach der Qualität ihres Zustandekommens beurteilt werden, nicht nach ihrem Ausgang.

Innerhalb einer risikobewussten Kultur besteht ein gegenseitiges Risikoverständnis. Dies bedeutet, dass jede Person in einem Betrieb, von den Mitarbeitern bis zu der Betriebsleitung, gemeinsame Grundwerte und Überzeugungen hat. Ein gemeinsames Risikoverständnis sollte jedoch nicht unterschiedliche Sichtweisen und Haltungen in der Belegschaft blockieren, sondern Diversität fördern. Die Mitarbeiter sollten ihre Meinungen austauschen und sich gegenseitig hinterfragen. Dies erweitert den Denkhorizont und ermöglicht vielfältige Blicke auf Sachverhalte und Risiken bzw. eine tiefgründige Risikoabwägung. Um eine solche Kultur zu entwickeln, sollten mehrere Aspekte erfüllt werden. Es müssen zunächst die Risiken des Betriebs, die sich aus den wirtschaftlichen Aktivitäten ergeben, identifiziert werden. Die Risiken müssen darüber hinaus auf die unterschiedlichen Unternehmensbereiche, Geschäftsfelder, Sortimente und Produkte des Betriebs unterteilt werden. Des Weiteren sollten die Praktiken und Aufgaben des Risikomanagementprozesses klar beschrieben sein.

4.2 Vorgelebte Risikokultur: Risiken kontrollieren und kommunizieren

Der Umgang mit Risiken im Betrieb erfolgt im Risikomanagement. Hierunter versteht man grundsätzlich die Gesamtheit aller Maßnahmen zur Analyse, Steuerung und Überwachung von Risiken, die einen Betrieb aktuell oder potenziell treffen können. Die Geschäftsleitung ist dafür verantwortlich, dass alle Aufgaben zum Risikomanagement ausge-

führt werden. Dazu muss es diese in der Organisation und in die Prozesse verankern. In jeder Phase und jedem Prozess sind die entsprechenden Mitarbeiter involviert. Es sollte sichergestellt werden, dass sich das Risikoverhalten der Mitarbeiter an dem vorgegebenen Wertesystem und Verhaltenskodex orientiert. Nur so wird die Risikokultur im Betrieb auch „gelebt“. Die Risikokultur kann im Betrieb einheitlich vertreten sein, wenn ein geeigneter organisatorischer Rahmen geschaffen wird. Die Organisation des Risikomanagementsystems ist daher ein entscheidender Faktor in der erfolgreichen Umsetzung der Risikokultur. Die Gesamtheit aller Aufgaben, Regelungen und Träger des Risikomanagements wird als Risikomanagementsystem bezeichnet und umfasst im weiteren Sinne alles im Betrieb, was sich mit Risiken befasst. Um zu gewährleisten, dass man einen effektiven Rahmen geschaffen hat, benötigt es der laufenden Überwachung und Kontrolle. Neben der Organisation, ist auch die Kontrolle der Prozesse und Abläufe ein entscheidender Faktor im betrieblichen Risikomanagement. Innerhalb der aktiven Risikomanagementprozesse und der anschließenden Kontrolle ist eine effektive Kommunikation unverzichtbar, da ansonsten wichtige Informationen zu Risiken gar nicht oder fehlerhaft weitergeleitet werden. Die Risikoberichterstattung im Betrieb erfolgt zwischen verschiedenen Bereichen und Mitarbeitern. Es kann zu unterschiedlichen Kommunikationsproblemen kommen. Man sollte sich im Klaren darüber sein, wie die Kommunikation ausgestaltet sein soll, welche Probleme dabei auftreten können und welche Verbesserungsansätze sich daraus ergeben. Ein optimales betriebliches Risikomanagement ist geprägt durch eine klare Organisation mit einer substanzialen Kontrolle und effektiven Kommunikationsstrukturen.

4.2.1 Risikomanagement der Neuzeit: Systematisch und dynamisch

Eine Risikomanagementorganisation wird aufgebaut, um systematisch und kontinuierlich mit den betrieblichen Risiken umzugehen. Es sollte sich an die sich verändernden Rahmenbedingungen regelmäßig anpassen. Diese Veränderungen haben eine zunehmende Komplexität der Aufgaben und Abläufe zur Folge und führen zu Unsicherheiten bei der Entscheidungsfindung. Üblicherweise liegen die Ziele des Risikomanagements in der Sicherung des Unternehmensfortbestandes, des zukünftigen Erfolgs, die Steigerung des Marktwertes sowie die Vermeidung oder Senkung der Risikokosten (vgl. Diederichs 2018, S. 12).

Das Risikomanagementsystem und alle damit verbundenen Maßnahmen können nur dann funktionieren, wenn sie fest in die **Geschäftsorganisation** eingebunden werden. Dies beginnt mit einer Verankerung des Systems in die Aufbauorganisation des Betriebs (vgl. Fleig 2018). Mitarbeiter brauchen das Risikomanagement nicht als eigenständiges organisatorisches und planerisches System verstehen. Es ist wichtig, dass das Risikomanagement mit den vorhandenen Systemen vernetzt wird (vgl. Gleißner 2019). Das bedeutet, dass zum einen die Informationen und Ergebnisse aus dem Risikomanagement und dem Controlling in die operativen und strategischen Planungen des Betriebs mit einfließen. Andererseits sollten bereits vorhandene Daten aus der Planung dem Risikomanage-

ment zur Verfügung gestellt werden. Diese Integration führt zu einer höheren Akzeptanz bei den Mitarbeitern.

Die **Risikokontrolle** bedient sich unterschiedlicher Verfahren zur Überwachung und aktuellen Bewertung der Betriebsrisiken. Auch hier führt ein organisatorischer Rahmen zu mehr Effizienz. Die Risikoüberwachung sollte so weit wie möglich in die vorhandenen Betriebssysteme implementiert und mit diesen verbunden werden. Die technisch orientierten Risiken können so jederzeit innerhalb der vorhandenen Prozesse in ihrer Entwicklung überprüft werden.

Ein weiterer Aspekt im Rahmen der Organisation des Risikomanagements ist eine nachvollziehbare, ordentliche und für Dritte verständliche Dokumentation (vgl. Gleißner 2019). Sämtliche Erkenntnisse über die Veränderung der Risikosituation sollten sinnvoll, einheitlich aufbereitet, dokumentiert und an die zuständigen Entscheidungsträger weitergeleitet werden. Ein disziplinierter und verantwortungsbewusster Umgang mit den Risiken reicht nicht aus, sofern es wesentliche Defizite in den Berichtswegen gibt. Dies bezieht sich vor allem auf eine risikoübergreifende, einheitliche Systematik der Risikobeschreibung und einem zusammenfassenden Risikobericht für die Geschäftsleitung. Der Bericht sollte über alle wesentlichen Risiken informieren. Zudem sollte er die Risiken in ihrer quantitativen und qualitativen Bedeutung zu den unterschiedlichen Bereichen des Betriebs zuordnen.

Für das Funktionieren eines Risikomanagementsystems ist es von entscheidender Bedeutung, dass die jeweiligen Aufgaben zugeordnet werden. Je zu überwachendem Risiko ist ein sogenannter „Risk Owner“ zu benennen, der allerdings nicht als „Risikoeigentümer“ übersetzt werden sollte. Der „Risikoverantwortliche“ hingegen kann bewirken, dass das Risiko tatsächlich innerhalb der bestimmten Vorgaben betrachtet wird. In diesem Zusammenhang muss in einem Betrieb insbesondere festgelegt werden, wie die Risikoverantwortlichkeit strukturiert ist (vgl. Gleißner 2019).

Neben einer klaren Aufgabenzuordnung ist es ebenso von Bedeutung, dass das Risikomanagement organisatorisch von der internen Revision getrennt wird. Das Risikomanagementsystem kann so von einer neutralen Stelle in seiner Leistungsfähigkeit geprüft werden.

4.2.2 Risikokontrolle: Eigenverantwortung plus Monitoring

Um die Aufgaben des Risikomanagements erfüllen zu können, ist der Aufbau einer Prozessüberwachung aller Phasen des Risikomanagements notwendig.

Die Kontrolle bzw. Überwachung stellt den letzten Schritt des Risikomanagements dar und kann als laufende Tätigkeit innerhalb des gesamten Prozesses des Risikomanagements angesehen werden. Eine zentrale Aufgabe der regelmäßig durchzuführenden Risikokontrolle ist es, die eingesetzten Messinstrumente und Steuerungsmaßnahmen in den vorgelagerten Schritten des Risikomanagements hinsichtlich ihrer Angemessenheit und Wirksamkeit zu überprüfen. Sofern Abweichungen zwischen tatsächlicher und geplanter Risikosituation festgestellt werden, ist es notwendig, diese hinsichtlich ihrer Ursachen zu

untersuchen und daraufhin wirksame Gegensteuerungsmaßnahmen zu entwickeln. Ebenso sollten auch Veränderungen der Informationen identifiziert werden, um sie in der Folgeperiode in den Prozess des Risikomanagements einfließen lassen zu können.

Die Risikoüberwachung bzw. das Monitoring umfasst daher die ständige Pflege und Verwaltung von Risiken. Daran angeschlossen ist die Ermittlung von Risikobehandlungsmaßnahmen. Diese Maßnahmen werden ebenfalls in ihrem Fortschritt und Abschluss in Form von Messungen kontrolliert. In den einzelnen Phasen des Risikomanagements werden Entscheidungen getroffen. Auch für eine Rückverfolgbarkeit der getroffenen Entscheidungen, ist die Zuordnung von Risikoverantwortlichen notwendig.

Wenn zum Beispiel eine Organisation mit dem Verkauf ihrer Produkte an neue Märkte in Übersee beginnt, werden sich neue Risiken für das Unternehmen ergeben. Es muss ein Überwachungsprozess vorhanden sein, um sicherzustellen, dass das Risikomanagementprogramm solche Änderungen berücksichtigt. Weitere Gründe für eine regelmäßige Risikokontrolle liegen unter anderem in der Erfüllung von Leistungszielen und der Zuteilung von Budgets. Das Monitoring kann Statistiken und Daten liefern, die zur Erfüllung gesetzlicher Verpflichtungen erforderlich sind. Dies umfasst beispielsweise Berichterstattungspflichten für Arbeitnehmer und Umweltschutzgesetze. Hierbei ist anzumerken, dass das Controlling in erster Instanz wiederum für das Monitoring aufbereitete Daten zur Verfügung stellt. Die wesentlichen Aktivitäten im Risikomanagementprozess müssen überwacht bzw. kontrolliert werden. Dies bezieht sich insbesondere auf Änderungen der allgemeinen Rahmenbedingungen, wie die organisatorischen Ziele, die Betriebsumgebungen, Gesetzesänderungen, Geschäftspläne oder die Stakeholder. Im Allgemeinen sind die Schwerpunkte des Überwachungsprozesses die Mitarbeiter, Produkte und Aktivitäten. Beispiele hierfür sind Änderungen in der Betriebsstruktur, Personalwechsel, Produktreklamationen, Arbeitsunfälle, Sachschäden, Betriebsunterbrechungen, Maschinenausfälle und andere Sicherheitsverletzungen. Die Durchführung der Risikokontrolle erfordert sowohl formelle als auch informelle Überwachungs- und Überprüfungsprozesse. Bei der formellen Überwachung werden Berichterstattungssysteme, wie monatliche oder vierteljährliche Schadensberichte im Zusammenhang mit versicherbaren Risiken eingerichtet. Das informelle Monitoring kann Diskussionen mit Mitarbeitern umfassen, Berichte auswerten und allgemeine Anfragen stellen. Einige Beispiele für formelle Überwachungssysteme für Risiken sind Anspruchsdatenbanken, Vermögensverlustberichte, Unfallberichte, Gesundheits- und Sicherheitsberichte am Arbeitsplatz oder die Verlängerung der Betriebsgenehmigung. Die Erfassung von Ursache, Zeit, Ort und Höhe der Verluste sowie anderer Informationen, die zur Analyse unerwarteter Ereignisse bzw. Verluste verwendet werden können, sollten ein wesentlicher Bestandteil jedes Überwachungssystems sein.

Im Allgemeinen sollten Mechanismen, unter anderem ein internes Kontrollsysteem (IKS), entwickelt und implementiert werden, um sicherzustellen, dass regelmäßige Überprüfungen stattfinden. Das oberste Management einer Organisation ist dafür verantwortlich, dass eine regelmäßige Kontrolle des Risikomanagementsystems gemäß den Vorgaben aus der Planung durchgeführt wird. Bei der Kontrolle der Aktivitäten des Risikomanagements ist es ebenfalls wichtig, die getroffenen Entscheidungen auf den einzelnen Ebenen

zu prüfen. Diese müssen logisch und effektiv sein. Zudem muss geprüft werden, ob die ergriffenen Maßnahmen wie erwartet funktionieren und die gewünschten Ergebnisse erzielen. Für jedes Risiko muss man sich im Klaren darüber sein, wie oft dieses kontrolliert werden muss, welche konkreten Ergebnisse aus der Überprüfung resultierten und wie die empfohlenen Maßnahmen im Fachbereich behandelt wurden.

Die Risikokontrolle kann grundsätzlich als eine laufende Überprüfung betrachtet werden, sie beinhaltet keine Steuerungsfunktion. Die aufgedeckten Schwächen im Risikomanagementprozess sind von dem zuständigen Risikoverantwortlichen zu bewältigen. Darüber hinaus lässt sich die Überwachung der Risiken neben formalen und informellen Prozessen, in prozessintegrierte und prozessunabhängige Kontrollen unterteilen. Die prozessintegrierten Überwachungsmaßnahmen knüpfen direkt an die Phasen der Risikoidentifizierung, -analyse, -bewertung und der in der Risikosteuerung ergriffenen Maßnahmen an. Das können Prozesskontrollen (Effizienz- und Wirksamkeitsprüfungen operativer Aktivitäten), Soll-Ist-Vergleiche, Überprüfungen von Risikokennzahlen sowie die Sicherstellung der Verwendung einheitlicher Risikomessmethoden sein. Organisatorische Kontrollmaßnahmen auf operativer Ebene beinhalten unter anderem die Funktionstrennung, das heißt, das Eingehen und das Überwachen von Risiken liegt nicht in der Verantwortung einer Person. Zudem gibt es weitere mögliche Maßnahmen, wie das Einrichten des Vier-Augen-Prinzips oder Zugangskontrollen bzw. Zugriffsberechtigungen im IT-Bereich. Die prozessintegrierten Kontrollmaßnahmen werden in regelmäßigen Abständen von prozessunabhängigen Kontrollen untersucht. Die interne Revision ist eine solche unabhängige Kontrollfunktion, mit der Mängel in der Auf- und Ablauforganisation erkannt werden sollen, um diese dann an das oberste Management und dem Aufsichtsrat zu berichten. Das Ziel ist es, eine Verbesserung des Überwachungssystems zu erreichen. Innerhalb des „Three Lines of Defense“-Modells bildet die interne Revision die dritte Verteidigungslinie und hat damit eine zentrale Bedeutung für die Risikoüberwachung (vgl. Rohlfs 2018, S. 303 ff.). Abb. 4.1 gibt einen Überblick über die Ausgestaltung des „Three Lines of Defense“-Modells in einem Betrieb. Die erste Linie ist für die operative Umsetzung der Richtlinien aus der zweiten Verteidigungslinie verantwortlich. Die zweite Linie beinhaltet die zentralen Funktionen und erstellt Vorgaben für die operativen Prozesse. Die Prozesse werden hierdurch gesteuert und überwacht. Die zweite Linie ist zudem für die Berichterstattung, insbesondere hinsichtlich der Risikosituation, zuständig. Die Interne Revision als dritte Verteidigungslinie ist die objektive und unabhängige Prüfungsinstanz. Sie stellt eine direkte Unterstützung für die Unternehmensleitung dar. Es wird gewährleistet, dass die Risiken im Risikomanagementprozess wirksam identifiziert, bewertet und gesteuert werden. Das über der Geschäftsleitung angesiedelte Überwachungsorgan kann zum Beispiel der Aufsichtsrat sein. Die Risikokontrolle kann auch durch andere unabhängige Funktionen, wie den Abschlussprüfer oder den Aufsichtsrat durchgeführt werden. Das „Three Lines of Defense“-Modell skizziert daher ein funktionsfähiges Kontroll- und Überwachungssystem in einer Organisation.

Im Rahmen der Risikokontrolle muss man sich an Ergebnissen, Informationen und Fakten orientieren. Das Controlling verfügt über genaue diese Aspekte. Das Risikoma-

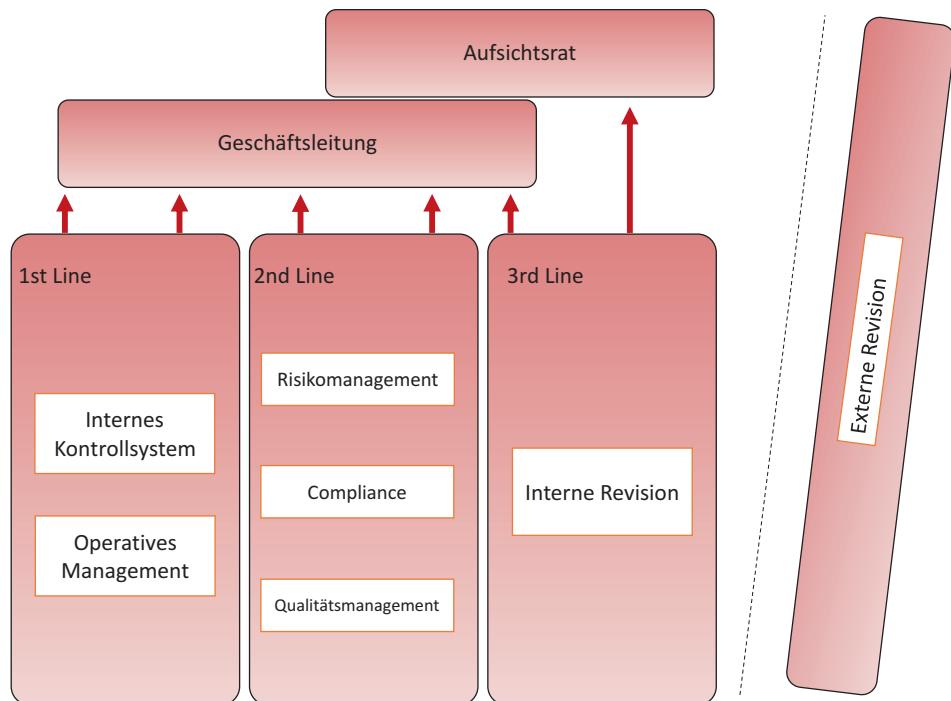


Abb. 4.1 Three-Lines-of-Defense-Modell. (Quelle: eigene Darstellung in Anlehnung an Chartered Institute of Internal Audit. <https://www.iiia.org.uk/resources/audit-committees/governance-of-risk-three-lines-of-defence>. Zugegriffen am 10.06.2019)

nagement weist eine deutliche Verzahnung zum Controlling auf, da aus der Notwendigkeit des Aufbaus eines Risikomanagements im Betrieb zusätzlich neue Aufgaben für ein Risikocontrolling abgeleitet werden können.

4.2.3 Kommunikation von Risiken für mehr Entscheidungsqualität

Das Management und die zuständigen Entscheidungsträger benötigen aktuelle und zuverlässige Informationen. Ein vollständiger Informationsfluss bildet die Grundlage für rationale und objektiv nachvollziehbare Entscheidungen. Informationen bilden die Basis für fundierte Entscheidungen und reduzieren das Risiko von als nachträglich erachteten Fehlentscheidungen. Damit sind Informationen über Risiken, insbesondere das Melden von Risiken, für die Existenz- und Erfolgssicherung unverzichtbar. Wer Informationen generiert, trägt daher eine hohe Verantwortung. Informationen sind von Qualität, wenn sie ausreichend, verlässlich, relevant und nützlich sind. Dies setzt voraus, dass man die Risiken in seinem Verantwortungsbereich kennt und in ihrer Wirkung versteht. Der Informationsfluss über Risiken hängt neben der organisatorischen Ausgestaltung der Berichtswägen

auch von der betrieblichen Risikokultur bzw. des Risikobewusstseins der einzelnen Mitarbeiter ab.

► **Risikokommunikation:** Jegliche Form der Berichterstattung über Risiken. Für eine nachhaltige Risikohandhabung ist ein möglichst transparenter und vollständiger Informationsfluss über Risikosituationen notwendig.

Von den Mitarbeitern eines Betriebs, unabhängig von ihrer Position oder organisatorischen Einheit, sollten die Identifizierung und Bewertung der Risiken ausgehen. Es ist wichtig, eine Risikokultur zu etablieren, durch welche die Risikophilosophie des Betriebs nachhaltig umgesetzt werden kann. Die betriebsindividuelle Risikokultur bestimmt die Ausgestaltung und den Ausführlichkeitsgrad der Risikoberichte. Die Risikoberichterstattung soll in nachvollziehbarer und aussagefähiger Art verfasst werden. Eine Integration aller Betriebsebenen und -einheiten in diesen Prozess ist in der Umsetzung nur durch eine entsprechende Risikokommunikation und Berichterstattung möglich.

Es ist wichtig, dass eine vollständige und reibungslose Kommunikation in den internen Bereichen vorhanden ist, um einen nachhaltigen Risikoumgang zu gewährleisten. Die interne Berichterstattung kann vielfältig sein und entsprechend der Zielsetzung der Informationen variieren. Verschiedene Berichtsarten sind vorstellbar. Dies kann eine Risikobeschreibung, ein Risikokatalog oder ein Gesamtbericht über das Risikoprofil sein. Für eine effektive Risikokommunikation ist es notwendig, ein Verständnis über die Inhalte und Abläufe der Risikoberichterstattung zu entwickeln. Man sollte sich der Probleme, die aus einer fehlerhaften Berichterstattung entstehen können, bewusst sein und Verbesserungsansätze hierfür finden (vgl. Aeschimann 2009, S. 1). Im Folgenden wird der Fokus auf der internen Risikokommunikation im betrieblichen Risikomanagement liegen.

4.2.3.1 Risikokommunikation ist Wissenskommunikation

Die adäquate und systematische Kommunikation über Risiken und die vorhandenen Fähigkeiten im Risikomanagement sind für jede größere Betriebseinheit entscheidend. Die Implementierung umfassender Risikomanagement-Strukturen reicht nicht aus, sofern keine funktionierenden Kommunikationsstrukturen in der Organisation vorhanden sind (vgl. Aeschimann 2009, S. 1). Eine fehlerhafte Risikokommunikation bzw. Reporting wirkt sich im gleichen Zuge auch auf die erfolgreiche Umsetzung der Risikokultur aus. Dies kann unter anderem an fehlendem Überblick über die Gesamtheit der Risiken oder der unzureichenden Verbreitung von Risikoberichten liegen. Des Weiteren kann es darin begründet sein, dass die verschiedenen Risikomanagement-Funktionen ihre Erkenntnisse ungenügend diskutiert und analysiert haben. Zudem können ähnliche Probleme, wie bei der Ausgestaltung des Risikomanagementsystems, auftreten. Wegen hoher Komplexität und Unvollständigkeit der internen Risikoberichterstattung, veralteter Daten oder der Verteilung der Berichte an die falschen Empfänger, kommt es zu ineffektiven Berichtswegen (vgl. Aeschimann 2009, S. 2).

Es ist notwendig, dass Organisationen systematische Kommunikationskonzepte für das Risikomanagement implementieren. Funktionierende Risikokommunikation kann im Sinne einer „Wissenskommunikation“ verstanden werden, die als „absichtlicher Transfer von Informationen, Erkenntnissen oder Erfahrungen über einzelne Risiken ... und Risikomanagement-Aktivitäten durch verbale und non-verbale Kommunikation“ definiert wird (vgl. Aeschimann 2009, S. 3). Dabei handelt es sich nicht nur um den Austausch von Daten und Fakten, sondern auch um Grundannahmen, Sichtweisen, Eventualitäten und Einschätzungen. Ziel ist es, dem Empfänger der Informationen dieses Wissen und eigene Ansichten zu vermitteln. Die Risikokommunikation kann als interaktiver Austauschprozess von Informationen und Meinungen zwischen einzelnen Verantwortlichen, Gruppen und Bereichen verstanden werden. Innerhalb dieses Prozesses geht es ebenfalls um das Festlegen von organisatorischen Maßnahmen zur Handhabung der Risiken. Ein wesentliches Ziel einer optimalen Risikokommunikation sollte eine Verbesserung des Verständnisses der Risiken und der damit verbundenen Risikomanagement-Prozesse sein. Zudem ist ein Hauptziel der Kommunikation im Risikomanagement, dass die Sichtweisen der relevanten Anspruchsgruppen mit einbezogen werden. Darüber hinaus wird angestrebt, dass durch eine vorhandene Kommunikationsstruktur sich alle Beteiligten ihrer Rollen und Verantwortlichkeiten bewusst sind.

Abb. 4.2 zeigt eine mögliche Struktur der Risikokommunikation innerhalb des Risikomanagements in einer Organisation. Dabei werden die wesentlich beteiligten Funktionen und ihre jeweiligen Kommunikationsbeziehungen dargestellt. Zu Beginn werden von dem Aufsichtsrat eine Grundausrichtung des Risikomanagements und möglicherweise Limite für einzelne Risiken festgelegt. Dabei diskutiert die Geschäftsleitung mit dem Aufsichtsrat die wesentlichen Risiken der Organisation. Die Geschäftsleitung erhält von den verant-

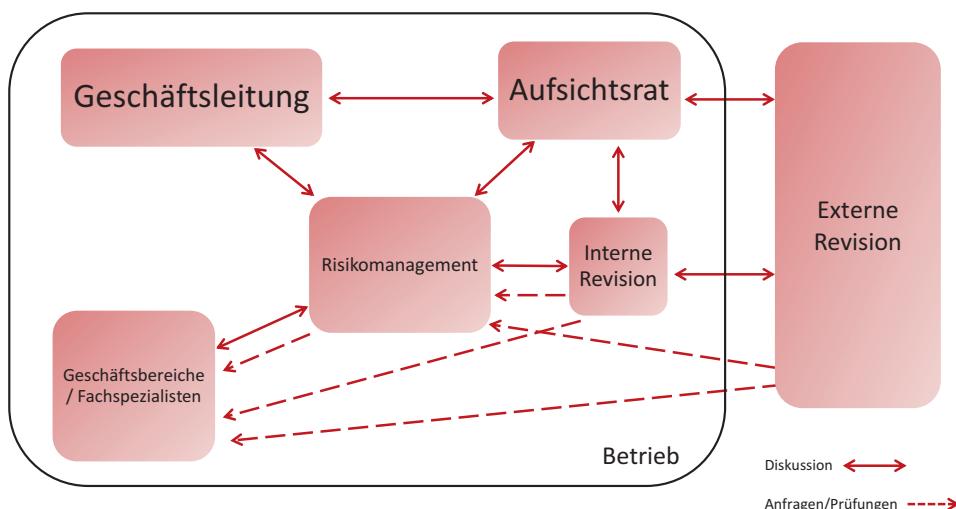


Abb. 4.2 Struktur der Risikokommunikation. (Quelle: eigene Darstellung in Anlehnung an Aeschimann 2009, S. 4)

wortlichen Personen der Geschäftsbereiche die risiko-relevanten Informationen bzw. prüft die jeweiligen Risikoeinschätzungen. In Form einer „second opinion“ unterstützen Fachspezialisten aus dem Controlling, der Rechtsabteilung oder anderen zentralen Supportfunktionen mit ihrer Einschätzung die Geschäftsleitung dabei. Im Gegenzug unterstützt das Risikomanagement die Geschäftsleitung und die einzelnen Geschäftsbereiche in den einzelnen Phasen des Risikomanagement-Prozesses (vgl. Aeschimann 2009, S. 4).

Die unabhängige Interne Revision überprüft im Auftrag des Aufsichtsrates die Effektivität und Effizienz der Geschäftsprozesse. Dies führt zu einer nachhaltigeren Risikokommunikation innerhalb der durchgeführten Prozesse.

Es besteht oftmals auch ein Interesse von externen Anspruchsgruppen für das Risikoprofil und die Risikophilosophie der Organisation sowie die gewählten Methoden im Rahmen des Risikoumgangs. Dies können neben Kunden und Fremdkapitalgebern, auch Regulatoren bzw. öffentliche Behörden sein (vgl. Aeschimann 2009, S. 4). Auf die Kommunikationsbeziehungen, die sich aus den Informationsbedürfnissen der Stakeholder ergeben, wird in diesem Kontext nicht genauer eingegangen.

Innerhalb der Risikokommunikation gibt es verschiedene Instrumente und Kompetenzen, die Unterstützung für die richtige Umsetzung leisten. Dabei geht es insbesondere um die Einhaltung einer einheitlichen Risikosprache. Eine gemeinsame Risikokultur ist die Voraussetzung für eine effektive Risikokommunikation.

Diese beginnt mit der Geschäftsleitung, die in Form von formalen Risikoausschüssen das Risikoprofil der Organisation beurteilt, genehmigt und überwacht (vgl. Aeschimann 2009, S. 5). Zudem legt sie Schwerpunkte des Risikomanagements fest. Innerhalb der Prozesse des Risikomanagements schaffen konsistente Analysen und Bewertungen von Einzelrisiken ein klares Verständnis der Konzepte des Risikomanagements. Darüber hinaus ist es möglich, über ein Risikokomitee ein ganzheitliches Bild über das Risikoprofil zu erhalten und bereichsübergreifende Maßnahmen festzulegen. In diesen Sitzungen nehmen Mitarbeiter aus den unterschiedlichen Geschäftsbereichen und Supportfunktionen teil. Ein entscheidendes Element innerhalb der Kommunikation von Risiken stellen die regelmäßigen Risikoberichte dar. Diese informieren über die Einzelrisiken und geben Aufschluss über die Entwicklung der Risiken. In diesem Rahmen können auch Lücken im Kontrollsysteem festgestellt werden. Eine hohe Effizienz der Kommunikation wird zudem durch vordefinierte Eskalationsprozesse sichergestellt. Im Falle eines Risikoeintritts sollte in allen betroffenen Bereichen Klarheit über die konkrete Vorgehensweise und Maßnahmeneinleitung herrschen (vgl. Aeschimann 2009, S. 5).

4.2.3.2 Es bleibt menschlich: Probleme der Risikokommunikation

Für die Analyse von Kommunikationsproblemen bzw. -barrieren im Risikomanagement kann man sich auf die folgenden drei Hauptakteure beschränken. Diese sind der Fachspezialist, der Risikomanager und die Geschäftsleitung. Dabei sind Risikomanager nicht nur im engeren Sinne als Mitarbeiter aus dem Risikomanagement-Bereich zu verstehen, sondern auch aus anderen Funktionen, wie dem Controlling, Qualitätsmanagement oder der Rechtsabteilung. Auch die Mitarbeiter aus diesen Funktionen haben unter anderem die

Aufgabe die Risiken der Organisation zu analysieren, zu überwachen und darüber zu berichten (vgl. Aeschimann 2009, S. 6).

Die Risikomanager unterstützen die Geschäftsleitung und die einzelnen Bereiche bei der Risikobewertung. In der Zusammenarbeit zwischen dem Risikomanagement und den Geschäftsbereichen kann es jedoch zu Zielkonflikten und Missverständnissen kommen. Die Kommunikation kann gestört werden, falls keine gemeinsame Risikosprache vorhanden ist. Fehlt es beispielsweise an breit akzeptierten Risikomodellen, einheitlichen Berichtsvorlagen oder auch klaren Begriffsdefinitionen, entstehen Unklarheiten und Missverständnisse.

Zielkonflikte entstehen, falls Vorgaben der Geschäftsleitung nicht im Einklang mit den Incentivierungen der Mitarbeiter stehen. Bei einer hohen Gewinnerwartung müssen die Mitarbeiter in den betroffenen Bereichen möglicherweise hohe Risiken eingehen. Dürfen sie das nicht wegen gleichbleibendem Sicherheitsinteresse, werden die Risikomanager auf derartige konkurrierende Ziele hinweisen. Ebenfalls müssen bei einem Ruf nach mehr Innovation oder Unternehmertum seitens der Geschäftsführung auch Fehler und Scheitern zugelassen werden. Bei unverändertem Rechtfertigungsdruck verstummt ansonsten die Forderung. Abhängig von der Risikostrategie fördert oder kritisiert das Risikomanagement das Eingehen von Risiken.

Langfristig können diese Konflikte zu einer nachhaltigen Störung der Kommunikation zwischen den Geschäftsbereichen und den Risikomanagern führen. Es kann dazu kommen, dass ein Mitarbeiter im Fachbereich relevante Daten und Informationen gegenüber dem Risikomanagement verschweigt, da er sich in seinem unternehmerischen Handeln eingeschränkt fühlt. Es ist zu erkennen, dass die Vorgaben und Entscheidungen aus der Geschäftsleitung negative Auswirkungen auf die Risikokommunikation haben können bzw. in einem sehr engen Zusammenhang mit der Risikokontrolle und -kultur stehen.

Darüber hinaus führt fehlende Kompetenz des Fachspezialisten oder des Risikomanagers zu Kommunikationsproblemen. Werden die Risiken und Geschäftsvorgänge wegen mangelndem Fachwissen der zuständigen Mitarbeiter nicht verstanden oder nicht bewertet, kann auch keine ordentliche Analyse und Diskussion darüber erfolgen. Teilweise werden Großrisiken nicht dokumentiert, für die Rückstellungen gebildet werden sollten oder man möchte sich nicht Produkthaftungsklagen exponieren. Dies erschwert eine ganzheitliche Sicht auf die Risiken.

Innerhalb der Prozesse der Risikoidentifizierung und -bewertung wird meist eine hohe Anzahl an relevanten Faktoren aufgeführt, die zudem untereinander in einer Beziehung stehen und sich gegenseitig beeinflussen. Dieses komplexe Zusammenspiel der Risikofaktoren kann dazu führen, dass die zuständigen Risikomanager oder Fachspezialisten die Übersicht und die Fokussierung auf die relevanten Aspekte verlieren. Für eine verbesserte Kommunikation über die wesentlichen Treiber und Zusammenhänge, sollten daher Visualisierungstechniken oder andere Instrumente genutzt werden (vgl. Aeschimann 2009, S. 7).

Aber auch innerhalb des Risikomanagements selbst kann es zu Kommunikationsproblemen kommen. Sofern die Bereichsleiter der verschiedenen Risikomanagement-Funktionen unabhängig voneinander arbeiten, kann es dazu führen, dass der Informationsaustausch erschwert wird. In der Folge sind einzelne Themengebiete nicht optimal abgedeckt.

Weitere Quellen für eine ineffektive Risikokommunikation sind fehlende Daten, Qualitätsmängel oder gar keine IT-Verarbeitungssysteme zur Risikoberechnung. Diese Faktoren führen dazu, dass keine aussagekräftigen Analysen und Risikoberichte erstellt werden können. Aber auch falls die Infrastruktur gegeben ist, können unpassende Modelle oder falsche Grundannahmen eine objektive Beurteilung der Risiken erschweren (vgl. Aeschimann 2009, S. 8).

4.2.3.3 Vernetzung und Verständlichkeit als Ausweg

Die oben genannten Aspekte in Bezug auf Kommunikationsprobleme innerhalb einer Organisation oder der einzelnen Funktionen und Bereiche sind keinesfalls vollständig und betreffen jeden Betrieb in einer anderen Art und Weise. Jedoch kann man aus den obigen Problemansätzen zentrale Ansatzpunkte für eine Verbesserung der Risikokommunikation ableiten.

Zum einen ist dies die Optimierung der Risikomanagement-Organisation. Für eine intensive Kommunikation und einem effektiven Wissensaustausch sollten Bereiche, die von dem gleichen Risiko betroffen sind, nah beieinander arbeiten bzw. gut miteinander vernetzt sein. Es geht dabei insbesondere um eine Regelung der Verantwortlichkeiten und das Einbeziehen aller Funktionen, auch kleinerer Supportbereiche, in die Entscheidungsfindung (vgl. Aeschimann 2009, S. 10).

Zudem muss natürlich eine risikobewusste Kultur gepflegt werden, um eine gemeinsame Risikosprache sowie offene und direkte Diskussionen von Chancen und Gefahren zu gewährleisten. Des Weiteren sollte eine ganzheitliche Sicht der Risikosituation angestrebt werden. Man darf sich, innerhalb der vermeintlich wichtigen finanziellen Risiken, nicht zu sehr ins Detail verlieren, sondern sollte sich auch auf die Bedeutung anderer Risiken konzentrieren. Dabei geht es vor allem um strategische Risiken und Reputationsrisiken, die schwerer zu bewerten sind.

Zuletzt ist als zentraler Aspekt die Verbesserung der vorhandenen Kommunikationsstrukturen zu nennen. Die internen und externen Instrumente wie Risikoberichte, Risikoausschüsse und Eskalationsprozesse müssen kritisch hinterfragt und auf Optimierungsmöglichkeiten untersucht werden. Standardisierte Layouts und prägnante Zusammenfassungen führen bei den Risikoberichten zu mehr Akzeptanz. Aber auch bei den organisatorischen Strukturen der Berichterstattung und der Berichtswege sollte man immer das Ziel von höherer Effektivität und Effizienz vor Augen haben. Es können beispielsweise Risikokoordinatoren zwischen verschiedenen Bereichen zur besseren Abstimmung eingesetzt werden (vgl. Aeschimann 2009, S. 10).

4.3 Fazit: Risikokultur verkörpert gelebte Risikostrategie

Die Risikokultur hat eine große Bedeutung für den nachhaltigen Erfolg eines Betriebs, denn diese hat einen Einfluss auf die unternehmerischen Entscheidungen und damit dem zukünftigen Unternehmensbestand. Es muss von Beginn an klar sein, welche Grundsätze und Ziele man mit der Risikokultur verfolgen möchte. Eine Grundlage für die Risikokul-

tur bietet die Risikostrategie des Betriebs. Die Risikokultur sollte im gesamten Betrieb gemäß des vorgegebenen Wertesystems etabliert und gelebt werden. Das Risikobewusstsein der verantwortlichen Mitarbeiter sollte mit der betrieblichen Risikokultur übereinstimmen, damit zu jeder Zeit und in jedem Bereich risikoadäquate Entscheidungen getroffen werden können.

Für eine erfolgreiche Umsetzung der Risikokultur benötigt es eine funktionierende Organisation des Risikomanagements. Das Risikomanagementsystem kann als Rahmen dafür angesehen werden. In dem Risikomanagementsystem sollten die Risiken richtig eingeschätzt und entsprechend kommuniziert werden. Dies ermöglicht eine effektive und nachhaltige Entscheidungsfindung auf allen betrieblichen Ebenen.

Die Prozesse des Risikomanagements müssen kontrolliert werden, um die Qualität des Systems sicherzustellen. Mittels der Risikokontrolle werden die Prozesse und letztlich die getroffenen Entscheidungen überprüft. Dies beinhaltet automatisch eine regelmäßige Überwachung der Einhaltung der Risikoleitlinien. Vollständige und zuverlässige Informationen ermöglichen das Treffen von richtigen Entscheidungen.

Für einen optimalen Informationsfluss im gesamten Risikomanagementprozess benötigt es klare Kommunikationsstrukturen. Die Risikokommunikation zieht sich durch alle Aspekte der Risikokultur und ist daher der ausschlaggebende Faktor für eine effektive und effiziente Risikokultur. Ohne eine adäquate Risikoberichterstattung und die damit einhergehende Transparenz über die Risiken können die Ziele und Aufgaben des Risikomanagements nicht erfüllt werden.

Die im Betrieb gelebte Risikokultur wirkt sich somit direkt auf die individuelle Risikobewertung, die Organisation des Risikomanagements, die Risikokontrolle und die Kommunikations- bzw. Informationsqualität aus und kann als wichtiger Faktor für eine erfolgreiche Unternehmensführung angesehen werden.

Literatur

- Aeschimann, M. (2009). Kommunikation im Risikomanagement: Der vernachlässigte Erfolgsfaktor. https://www.risknet.de/uploads/tx_bxelibrary/1247548130_Kommunikation%20im%20Risikomanagement%20-%2020090714.pdf. Zugegriffen am 01.06.2019.
- Chartered Institute of Internal Audit: Governance of risk. (2019). Three lines of defence. <https://www.iiia.org.uk/resources/audit-committees/governance-of-risk-three-lines-of-defence/>.
- Diederichs, M. (2018). *Risikomanagement und Risikocontrolling* (4. Aufl.). München: Franz Vahlen.
- Fleig, J. (2018). Risikomanagement im Unternehmen organisieren. <https://www.business-wissen.de/hb/risikomanagement-im-unternehmen-organisieren/>.
- Gleißner, W. (2019). Ratschläge für ein leistungsfähiges Risikomanagement. <http://www.risikomanagement.info/Ratschlaege-fuer-ein-leistungsfaehiges-Risikomanagement.300.0.html>. Zugegriffen am 01.08.2019.
- Hirschmann, S. (2015). Zehn Thesen zum Risikomanagement der Zukunft. https://www.dvfa.de/fileadmin/downloads/Finanzakademie/CRM/Zehn_Thesen_zum_Risikomanagement_der_Zukunft_diebank_02_2015.pdf. Zugegriffen am 10.12.2019.

- Rohlf, T. (2018). *Risikomanagement im Versicherungsunternehmen* (2. Aufl.). Karlsruhe: VVW GmbH.
- Rosenkranz, F., & Missler-Behr, M. (2005). *Unternehmensrisiken erkennen und managen* (1. Aufl.). Heidelberg: Springer.
- Taleb, N. N. (2018). *Das Risiko und sein Preis – Skin in the Game*. München: Penguin.
- The Institute of Risk Management. (2012). *Risk culture*. London. https://www.theirm.org/media/885907_Risk_Culture_A5_WEB15_Oct_2012.pdf. Zugriffen am 01.07.2019.

Benedikt Hintze ist Wirtschaftsingenieur, MBA und Certified Internal Auditor. Als Leiter Versicherung & Senior Referent Risikomanagement beim Stahlerzeuger Georgsmarienhütte Holding GmbH wirkt er entscheidend mit an den Risikostrategien und Versicherungskonzepten der Geschäftsbereiche. Davor war er in vergleichbarer Funktion tätig beim Saatgutproduzenten KWS SAAT SE und beim Kunststoffverarbeiter Pöppelmann GmbH & Co. KG. Benedikt Hintze ist Delegierter im Gesamtverband der Versicherungsnehmenden Wirtschaft e. V., Seminarleiter sowie Autor von Fachartikeln zum Risikomanagement und des Buchs „Versicherungsmanager überzeugt Unternehmenschef“.

Philipp Beuker studierte Versicherungswesen mit den Schwerpunkten Risikomanagement, Sachversicherung und Personalwesen am Institut für Versicherungswesen der Technischen Hochschule Köln. Im Anschluss absolvierte er dort auch das Masterstudium Risk & Insurance. Vor dem Studium schloss er eine Ausbildung zum Kaufmann für Versicherungen und Finanzen bei der LVM Versicherung ab. Als Nebentätigkeit arbeitete er während des Studiums bei der LVM Versicherung im Schadenmanagement und im Bereich für „Assistanceleistungen“.

Teil III

Betriebliches Risikomanagement



Klassische Risiken im Überblick

5

Daniel Aschoff und Julian Heitmann

Zusammenfassung

Die Risikolandschaft in der Industrie ist vielfältig und befindet sich stetig im Wandel. Aufgrund der Digitalisierung sowie der zunehmenden Globalisierung, verändern sich die Risikoprofile der klassischen Risiken wie Feuer, Naturkatastrophen, Haftungsschäden oder Betriebsunterbrechungen rasant. Daneben entstehen aber auch neue Risiken wie Cyberkriminalität oder Datenschutzverstöße. Global betrachtet herrschen zwischen den Risikolandschaften der einzelnen Länder viele Gemeinsamkeiten, dennoch sind signifikante Unterschiede festzustellen. Die Industriever sicherung steht vor großen Herausforderungen. Zum einen kämpft sie in einzelnen Sparten mit der Profitabilität des Marktes und befindet sich mittlerweile auf der Schwelle zur Marktverhärtung. Der intensive Wettbewerb verhindert jedoch zumeist flächendeckende Preissteigerungen. Eine weitere Aufgabe liegt in der Reduzierung der weltweiten Deckungslücke, welche nicht nur in den sogenannten Emerging Markets zu finden ist, sondern auch in Regionen mit einer hohen Versicherungsdurchdringung.

D. Aschoff (✉)

Allianz Global Corporate & Specialty SE, München, Deutschland

E-Mail: Daniel.Aschoff@allianz.com

J. Heitmann

TH Köln, Institut für Versicherungswesen, Köln, Deutschland

E-Mail: heitmann.julian@gmx.de

5.1 Einleitung

Der Begriff des Risikos beschreibt die möglichen negativen Auswirkungen von unternehmerischen Entscheidungen. Das Eingehen von Risiken ist im Wirtschaftsleben unvermeidbar, weshalb ein planvoller Umgang durch das Risikomanagement sinnvoll erscheint. Das Risikomanagement identifiziert, analysiert, bewertet und steuert sämtliche Risiken, denen ein Unternehmen ausgesetzt ist. Die Steuerung von Risiken kann unter anderem mithilfe der Versicherungswirtschaft vollzogen werden, indem insbesondere existenzbedrohende Risiken transferiert werden. Hierbei handelt es sich überwiegend um Risiken, deren Eintrittswahrscheinlichkeit gering ist, ihr Schadenausmaß jedoch besonders hoch sein kann. Dieses Kapitel befasst sich mit den klassischen Industrierisiken und den Entwicklungen des Industriever sicherungs marktes. Im ersten Abschnitt sollen die klassischen Risiken eines Industrieunternehmens systematisiert werden und Ursachen, sowie Risikophänomene herausgearbeitet werden. Im Anschluss folgt eine Analyse der Marktentwicklung aus unterschiedlichen Blickwinkeln. Zuerst werden die Entwicklungen der letzten Jahre aus Sicht der Industrie näher betrachtet werden. Dabei werden sowohl die zeitlichen Veränderungen der größten Risiken, als auch regionale Unterschiede herausgearbeitet. Anschließend erfolgt eine Untersuchung der Marktentwicklung aus Sicht der Versicherungswirtschaft. Der Fokus liegt hier insbesondere auf der Profitabilität des Marktes und befasst sich mit der Frage, ob sich der Industriever sicherungs markt auf der Schwelle zur Marktverhärtung befindet. Im Anschluss wird das Problem der sogenannten Deckungslücke, also dem Unterschied zwischen den entstandenen wirtschaftlichen und den versicherten Schäden, analysiert und entsprechende Maßnahmen abgeleitet.

5.2 Überblick klassische Risiken

Industrierisiken können anhand verschiedener Kriterien systematisiert werden, welche in Abb. 5.1 dargestellt sind. Die Ursache eines Industrierisikos kann endogen oder exogen sein. Endogene Ursachen entstehen aus dem Inneren eines Systems heraus. So kann das Versagen von menschlichem Handeln oder fehlerhafter Technik bestimmte Risiken nach sich ziehen. Als klassisches Beispiel dieser sogenannten Man-made Risiken sei das Feuer risiko zu nennen. Im Gegensatz hierzu wirken die exogenen Ursachen von außen auf das System ein. Dies sind unter anderem Gefahren aus Naturkatastrophen, Wirtschaft oder Politik. Die Unterscheidung zwischen endogenen und exogenen Ursachen ist nicht immer eindeutig abgrenzbar und die Übergänge sind fließend, wie das Beispiel des Kriminalitätsrisikos verdeutlicht. Unternehmen können Schäden durch kriminelle Handlungen sowohl durch fremde Personen, als auch durch die eigenen Mitarbeiter erleiden. Die Möglichkeit der Einflussnahme auf exogene Risiken ist niedriger als auf endogene Ursachen, denn sie lassen sich nur begrenzt vermeiden. Dennoch lässt sich das potenzielle Schadenausmaß durch geeignete präventive Maßnahmen verringern. Ein weiteres Unterscheidungskrite-

Ursachen	Endogen: Mensch / Technik / Organisation Exogen: Naturkatastrophen / Kriminalität / Wirtschaft / Politik					
Risiko- phänomene	Wirken auf eigenes Leistungspotenzial				Wirken nach außen	
	Sachrisiken	Ertrags- risiken	Personen- risiken	Andere Risiken	Produkt- risiken	Umwelt- risiken
Versicherungsprodukte / Deckungen	Feuer Natur- gefährten All Risk	Betriebs- unter- brechung Mehr- kosten	Unfall Lebens- und Pensions- versicherung	Politische Risiken Kredit- risiken	Produkt- haftung Rückruf Transport- haftung	Abfälle Deponien

Abb. 5.1 Systematisierung von Industrierisiken. (Quelle: eigene Darstellung in Anlehnung an Brühwiler 1994, S. 25)

rium ist die Richtung ihrer Auswirkungskraft. Industrierisiken können zum einen das eigene Leistungspotenzial angreifen oder ihre Kraft nach außen wirken. So bedrohen Sach-, Ertrags- und Personenrisiken stets unmittelbar das Unternehmen, während Produkt- oder Umweltrisiken sich zunächst nach außen, also auf externe Dritte, auswirken und im Anschluss negative Folgen auf das eigene Unternehmen entwickeln. Im Schadenfall kann jedoch jedes einzelne Risiko die Leistungs-, Liefer- und Wettbewerbsfähigkeit sowie die finanzielle Lage des Unternehmens gefährden (vgl. Brühwiler 1994, S. 24 ff.).

5.2.1 Sachrisiken

Sachrisiken wirken sich unmittelbar auf die Vermögensgegenstände des Unternehmens aus, indem sie diese durch ihre physische Einwirkung beschädigen oder zerstören. Insbesondere existenzbedrohende Risiken, wie Gefahren aus Feuer, Naturkatastrophen oder Erdbeben stellen für Industrieunternehmen eine hohe Gefahr dar, weshalb sie besondere Priorität im Risikomanagementprozess genießen. Solche Risiken sind dadurch gekennzeichnet, dass ihre Eintrittswahrscheinlichkeit gering, ihr potenzielles Schadenausmaß hingegen äußerst hoch ist (vgl. Brühwiler 1994, S. 23 ff.).

Die Versicherungswirtschaft bietet unterschiedliche Lösungsansätze an, um diesen Risiken entgegenzutreten. Grundsätzlich werden in der Sachversicherung benannte Sachen, die sich auf dem Versicherungsgrundstück (und teilweise auch außerhalb) befinden, gegen einen Sachsubstanzzschaden versichert. Hierzu zählen insbesondere Gebäude, technische und kaufmännische Betriebseinrichtungen, Vorräte oder Geschäftsunterlagen. Die Versicherungswirtschaft bietet hier zwei Vorgehensweisen an, um Versicherungsschutz bereit-

zustellen. Entweder können einzelne Gefahren enumerativ aufgeführt werden oder das Versicherungsunternehmen bietet eine Allgefahrendeckung an. Letzteres hat sich in der Sachversicherung nicht durchsetzen können, während sie in der Transportversicherung sowie der Betriebs- und Produkthaftpflichtversicherung üblich ist (vgl. Mikosch 1991, S. 119 ff.).

Feuer

Ereignisse durch Feuer oder Explosionen stellen ein beachtliches Risiko für Unternehmen dar. Insbesondere die Industrialisierung und der technische Fortschritt haben dazu geführt, dass die Schadensummen sowie die Schadenhäufigkeiten in den vergangenen Jahren stetig zunahmen (vgl. Brühwiler 1994, S. 27 ff.). Im Jahr 2018 lag der durchschnittliche Schadenaufwand aus Ereignissen durch Feuer bei rund 1,5 Millionen Euro. Insgesamt sorgten Brände und Explosionen an Gebäuden oder Anlagen (Ausnahme Waldbrände) im Jahr 2018 für einen versicherten Schaden in Höhe von 14 Milliarden Euro (vgl. AGCS 2019, S. 19). Die häufigste Brandursache ist nach Angaben des Instituts für Schadenverhütung und Schadenforschung der öffentlichen Versicherer mit 33 Prozent Elektrizität, gefolgt von menschlichem Fehlverhalten mit 17 Prozent (vgl. GDV 2019). Tab. 5.1 zeigt einige prominente Vertreter von Großbränden aus den letzten Jahren.

Naturkatastrophen

Schäden durch Naturkatastrophen, sogenannte Elementarschäden, werden durch das Wirken der Natur hervorgerufen, also ohne menschliches Handeln. Dazu gehören Risiken durch Sturm, Hagel, Überschwemmung und Erdbeben. Anders als bei den sogenannten „man-made Risiken“ handelt es sich um exogene Risikoursachen, weshalb sie sich nicht aktiv vermeiden lassen. Dennoch können Unternehmen durch geeignete Schadenpräventi-

Tab. 5.1 Prominente Vertreter von Großbränden. (Quelle: eigene Darstellung in Anlehnung an GDV 2019)

Ereignis	Datum	Ursache	Folgen
Notre-Dame, Paris	15.04.2019	Mutmaßlich Bauarbeiten	Schätzung: Hunderte von Millionen Euro
Moorbrand, Emsland	03.09. bis 10.10.2018	Schießübungen der Bundeswehr setzten den Torf des Moorböden unterirdisch in Brand	Mind. 50 Mio. Euro und Zerstörung von 1000 Hektar Moor im Naturschutzgebiet
Grenfell Tower, London	14.06.2017	Defekter Kühlschrank im 4. Stock	71 Tote
BASF, Ludwigshafen	17.10.2016	Explosion nachdem eine Rohrleitung bei Arbeiten beschädigt wurde	Fünf Tote, 28 (teils) schwer Verletzte, Hoher BU-Schaden
Herzogin-Anna-Amalia-Bibliothek, Weimar	02.09.2004	Vermutlich defektes Elektrokabel	Schätzung: 67 Mio. Euro, Zerstörung von 50.000 historischer Werke

onsmaßnahmen, wie zum Beispiel die Standortwahl, Auswahl stabiler Bauarten oder Errichtung von Hochwasserschutzmauern, die Folgen aus diesem Risiko minimieren (vgl. Brühwiler 1994, S. 33 f.).

Stürme sowie Überschwemmungen können durch ihre immensen Auswirkungen existenzbedrohende Folgen für Unternehmen haben. Im Jahr 2017 verursachten die drei Stürme Harvey, Irma und Maria (HIM) einen wirtschaftlichen Schaden in Höhe von 217 Milliarden US-Dollar, wovon lediglich 91 Milliarden US-Dollar versichert waren (vgl. Swiss Re Institute 2018, S. 20). Aufgrund der enormen Folgen und mangelnder Einflussnahme in Bezug auf die Eintrittswahrscheinlichkeit, befindet sich dieses Risiko seit mehreren Jahren stets unter den größten fünf Risiken auf dem Allianz Risk Barometer.

Für Versicherungsunternehmen ist die Zeichnung solcher Risiken aufgrund der Gefahr von Kumulschäden besonders anspruchsvoll. Ein Kumulschaden tritt ein, wenn eine Vielzahl von unterschiedlichen Versicherungsnehmern durch ein einzelnes regionales Schadeneignis betroffen sind. Dies ist bei Naturereignissen regelmäßig der Fall, denn während ein Brand meist in einem konzentrierten Bereich wirkt, treten Naturkatastrophen in einem breit gestreuten Bereich auf. Um eine ausreichende Risikostreuung zu gewährleisten, müssen die Versicherer Risiken aus geografisch unterschiedlichen Regionen zeichnen und ihr Kumul ausreichend kontrollieren. Darüber hinaus ist die Schadenfrequenz, insbesondere beim Erdbebenrisiko, sehr gering, weshalb eine qualitativ hochwertige Datengrundlage kaum vorhanden ist. Eine solche Grundlage wird jedoch für eine verlässliche Kalkulation des Risikos benötigt (vgl. Czeremuga 2016, S. 3 ff.).

Warentransport

Beim Transport von Waren können Schäden aus Unfällen, Stürzen beim Auf- und Entladen oder Diebstählen auftreten. Hinzu kommen Spezialrisiken, welche sich aus der Eigenart einzelner Waren ergeben. Beispielsweise können bestimmte Waren durch Oxidation einen Sachschaden davontragen oder Lebensmittel werden durch Geruchsübertragung oder Ungeziefer ungenießbar. Außerdem muss die Kühl- und Gefrierkette beim Transport von Nahrungsmitteln eingehalten werden. Die einzelnen Schäden aus dem Warentransport weisen zwar keine außerordentlich hohen Schadensummen auf, treten dafür jedoch deutlich häufiger ein (vgl. Brühwiler 1994, S. 37 f.). Die Vielzahl an Risiken, die sich beim Warentransport ereignen können, machen deutlich, warum die Versicherungswirtschaft üblicherweise mit einer Allgefahrendeckung an den Markt geht.

5.2.2 Ertragsrisiken

Das Ertragsrisiko, insbesondere das Betriebsunterbrechungsrisiko, ist nach Angaben des Allianz Risiko Barometers das größte Risiko für Industrieunternehmen und befindet sich seit sieben Jahren in Folge auf Platz 1. Betriebsunterbrechungsschäden sind oft deutlich höher, als die reinen korrespondierenden Sachschäden. Im Jahr 2018 betrug der durchschnittliche Schadenaufwand rund 3,1 Millionen Euro und ist damit rund 39 Prozent höher

als der korrespondierende durchschnittliche Sachschaden mit 2,2 Millionen Euro (vgl. AGCS 2019, S. 8).

Während sich die Sachrisiken vordergründig auf die bilanzierbaren Vermögensgegenstände eines Unternehmens konzentrieren, beziehen sich Ertragsrisiken auf ertragswirksame Größen der Gewinn- und Verlustrechnung. Hierbei handelt es sich um Risiken aus der Produktionsstörung oder Betriebsunterbrechung.

Betriebsunterbrechungen entstehen traditionell durch einen Sachschaden, welcher einen Stau oder eine Unterbrechung im Produktionsprozess hervorruft. Voraussetzung für eine versicherte Betriebsunterbrechung ist ein versicherter Sachschaden auf dem im Versicherungsschein genannten Grundstück. Daneben gibt es zwei Spezialfälle, welche unter bestimmten Voraussetzungen versicherbar sind. Ist das Tochterunternehmen des Versicherungsnehmers Zulieferer für ein anderes Tochterunternehmen, dann kann die Betriebsunterbrechung auch ohne Eintreten eines Sachschadens versichert sein (Wechselwirkungsschaden). Neben den Wechselwirkungsschäden kann ein Unternehmen auch von den sogenannten Rückwirkungsschäden betroffen sein. Hierbei entsteht eine Betriebsunterbrechung aufgrund von Schäden, die außerhalb des betroffenen Unternehmens eintreten und zu einer Unterbrechung der Lieferkette führen (vgl. Mikosch 1991, S. 128 f.). Der Ausfall von wichtigen Zulieferern oder Kunden, welche eine besonders hohe Menge an Produkten abnehmen, sind hier kritische Faktoren (vgl. Brühwiler 1994, S. 39 ff.). Rückwirkungsschäden haben im Laufe der Zeit besonders an Bedeutung gewonnen. Die Globalisierung und internationale Vernetzung von Unternehmen, sowie die „Just-in-Time“ bzw. „Just-in-Sequence“ Lieferung führen zu einem erhöhten Risiko in diesem Bereich.

Neben diesen klassischen Risiken führen eine Reihe weiterer Risiken zu einem Anstieg von potenziellen Betriebsunterbrechungen. Viele dieser Risiken verursachen zwar keinen Sachschaden, dennoch kommt es häufig zu einer Störung des Betriebes. Der Zusammenbruch des IT-Systems, Produktrückrufaktionen, Cyberangriffe, Terrorangriffe oder politische Unruhen sind bedeutsame Risiken für Unternehmen, welche stets zu einer Unterbrechung der operativen Tätigkeit führen können (vgl. AGCS 2019, S. 10 ff.).

Aufgrund der Komplexität wird das Betriebsunterbrechungsrisiko in vielen Unternehmen oft unterschätzt. Es ist eine gewaltige Aufgabe alle Risiken zu erfassen und den Verlust hieraus zu kalkulieren. Besonders die Zusammensetzung der Lieferkette und der sich daraus ergebenen Rückwirkungsschäden stellt das Risikomanagement regelmäßig vor große Herausforderungen. Versicherungsunternehmen können hier, neben dem reinen Anbieten von Versicherungsschutz, unterstützend tätig werden, indem sie geeignete Tools zur Verfügung stellen. Diese Tools ermöglichen die Modellierung von Zusammenhängen zwischen den einzelnen Lieferketten und können entsprechende Verlustszenarien darstellen (vgl. AGCS 2019, S. 11).

5.2.3 Personenrisiken

Neben den Sach- und Ertragsrisiken besitzen Personenrisiken einen hohen Stellwert für Industrieunternehmen und Gesellschaft. Sie können in Form von Unfällen oder Berufskrankheiten auftreten. Deshalb sind in modernen Industriestaaten Maßnahmen, wie Unfallverhütung und Gesundheitsvorsorge nicht mehr wegzudenken. Dennoch lassen sich Unfälle auch bei höchsten Sicherheitsstandards nicht vermeiden, welche neben möglichen Reputationsrisiken auch erhebliche Schadenersatzansprüche zur Folge haben können. So wohl die soziale als auch die private Versicherungswirtschaft leisten einen nennenswerten Beitrag zur Finanzierung dieses Risikos (vgl. Brühwiler 1994, S. 42).

5.2.4 Andere Risiken

Neben den zuvor genannten Risiken gibt es weitere klassische Risiken, welche sich nicht in eine der oben genannten Gruppen einordnen lassen. Zu den Wichtigsten zählen Gefahren aus politischen Risiken und Kreditrisiken.

Politische Risiken

Für Industrieunternehmen spielen politische Risiken eine besondere Rolle. Im klassischen Sinne gehören hierzu Ereignisse wie Krieg, Bürgerkrieg, Enteignung oder Beschlagnahmung von Firmeneigentum durch staatliche Eingriffe (vgl. Brühwiler 1994, S. 45 ff.).

Politische Risiken ergeben sich aus dem Handeln von Regierungen oder politischen Gruppen. Sie können die Kosten des Unternehmens erheblich erhöhen und erschweren Langzeit-Investitionen sowie Handelsgeschäfte. Hierzu zählen insbesondere Ereignisse wie die politischen Unruhen oder Bürgerkriege wie in Syrien. Investitionen in diese Regionen können nur unter gewissen Unsicherheiten getätigt werden. Auch der Austritt der Briten aus der Europäischen Union führt auf der einen Seite zu immensen Kosten für alle Beteiligten, auf der anderen Seite lässt er aber auch die Zukunft über das Weiter bestehen der EU offen. Entsprechend schwierig gestaltet sich die Planung und zukünftige Strategie für im EU-Raum tätige Unternehmen (vgl. Aon plc 2017, S. 34 f.).

Die Erfassung und Quantifizierung dieser Risiken ist eine anspruchsvolle Aufgabe des Risikomanagements und kann durch verschiedene Herangehensweisen erfolgen. Das sogenannte Länderrisiko hilft in erster Instanz bei der Einschätzung des Exposure. Es wird bestimmt, indem unterschiedliche Wirtschafts- und sozio-politische Faktoren in einem Modell analysiert und zusammengefasst werden. Viele kommerzielle Anbieter und Rating Agenturen wie Fitch, Moody's und Standard & Poor's bieten solche Modelle zur Unterstützung an. Der Versicherungsmarkt verfügt über eine Reihe von unterschiedlichen Deckungskonzepten gegen politische Risiken (vgl. Federkeil 2016, S. 3 ff.).

Kreditrisiken

Das Kreditrisiko umfasst die Gefahr, dass ein Kreditnehmer seine Rückzahlungsverpflichtung nicht im vollständigen Umfang nachkommen kann. Hierbei wird zwischen dem Delkredrerisiko, also dem Ausfall von Forderungen bei Zahlungsunfähigkeit und dem Kautionsrisiko, welches Bürgschaften und Garantien umfasst, unterschieden. Die Versicherungswirtschaft leistet im Rahmen der Kreditversicherung Schadenersatz, sobald die vereinbarte Zahlungsfrist durch das Eintreten einer Insolvenz nicht eingehalten wird. Zusätzlich kann auch die einfache Nichtzahlung des Schuldners unter bestimmten Voraussetzungen abgesichert werden. Für Versicherungsunternehmen spielt im Rahmen der Kreditversicherung die Schadenverhütung eine besonders große Rolle. Aus diesem Grund findet regelmäßig eine gründliche Kreditwürdigkeitsprüfung durch den Versicherer statt (vgl. Mikosch 1991, S. 157 ff.).

Insbesondere transnationale Konzerne mit Tochterunternehmen im Ausland können den Kreditversicherungsmarkt für ihr Forderungsmanagement nutzen. Warenkreditversicherungen bieten Planungssicherheit und die kontinuierliche Bonitätsprüfung der Versicherer sorgt präventiv dafür, Schadensfälle zu minimieren (vgl. Wittgen 2017, S. 5).

5.2.5 Produktrisiken

Produktrisiken wirken sich nicht unmittelbar auf das Unternehmen aus, sondern zunächst auf eine dritte Partei. Durch fehlerhafte Produkte oder Dienstleistungen können, sofern ein Sach-, Personen- oder Vermögensschaden eingetreten ist, Haftungsansprüche entstehen. Der hieraus resultierende finanzielle Schaden kann erhebliche Summen fordern. Darüber hinaus besteht die Gefahr, dass durch Produktmängel und Rückrufaktionen großes Medieninteresse hervorgerufen wird und die Reputation des Unternehmens großen Schaden erleidet. Aufgrund der verschiedenen Rechtssysteme sind die Regelungen der Haftung zwischen den USA und der Europäischen Union recht unterschiedlich. Innerhalb Europas wurde durch die Einführung von Richtlinien eine Angleichung der Haftungssysteme geschaffen. Die deutsche Haftung kann in drei Kategorien eingeteilt werden – die Haftung aus § 280 BGB aufgrund eines Vertragsverhältnisses, die Haftung aus dem Produkthaftungsgesetz und die Haftung aus § 823 BGB aufgrund unerlaubter Handlungen (vgl. Klinkhammer 2017, S. 3 ff.).

Die Versicherungswirtschaft hat auf dieses Risiko reagiert, indem sie Betriebshaftpflicht-, Produkthaftpflicht- und Rückrufkostenversicherungskonzepte entwickelt hat. Die Haftpflichtversicherung befriedigt berechtigte Ansprüche Dritter (Schadenersatz) und wehrt unberechtigte Ansprüche ab. Sie ist eine Allgefahrendeckung und deckt Personen- und Sachschäden ab. Vermögensschäden, die sich als Folge von Personen- oder Sachschäden ergeben, sind ebenfalls gedeckt. Reine Vermögensschäden dagegen sind jedoch grundsätzlich ausgeschlossen (vgl. Mikosch 1991, S. 96 ff.).

Die Bewertung des Haftungsrisikos gestaltet sich für das Risikomanagement des Unternehmens sehr schwierig. Insbesondere das Schadenausmaß wird oft unterschätzt, was bei der Auswahl des Versicherungsschutzes schnell zu einer Unterversicherung führen kann. Hinzu kommen weitere Aspekte der Digitalisierung und Globalisierung. Die vermehrte Vernetzung von Unternehmenszweigen, welche die Abhängigkeiten einzelner Unternehmen erhöht, lassen neue Risikoprofile entstehen. Hierauf müssen sowohl die Industrieunternehmen als auch die Versicherungswirtschaft angemessen reagieren und neue Konzepte entwickeln, um das Haftungsrisiko zu vermindern (vgl. Marsh GmbH 2019, S. 7).

5.2.6 Umweltrisiken

Die Bedeutung von Umweltschäden und die Haftung, die sich aus diesen Schäden ergibt, gewinnen in der Gesellschaft zunehmend an Bedeutung. Dies wird auch durch die im Jahr 2004 verabschiedete Richtlinie 2004/35 EG „Umwelthaftung zur Vermeidung und Sanierung von Umweltschäden“ durch das Europäische Parlament bzw. durch den Europäischen Rat deutlich. Deutschland hat die Richtlinie im Jahr 2007 durch die Einführung des „Umweltschadengesetzes“ umgesetzt. Die Anzahl der Schadensfälle ist bisher überschaubar und es existieren auch nur wenige Gerichtsurteile zu diesem Thema. Dennoch kann es aufgrund der öffentlich-rechtlichen Haftung für Umweltschäden zu erheblichen Sanierungsverpflichtungen kommen (vgl. Klinkhammer 2018, S. 6 ff.).

Umweltschäden sind in der Betriebs- und Produkthaftpflichtversicherung ausgeschlossen. Die Versicherungswirtschaft hat mit einer Umweltschadenversicherung auf die Situation reagiert und eine auf das Umweltschadengesetz zugeschnittene Deckung entwickelt (vgl. Mikosch 1991, S. 111 ff.).

5.2.7 Veränderung der Risikolandschaft

Im Laufe der Zeit hat sich ein starker Wertewandel in der Wirtschaft vollzogen, welcher sowohl das Risikomanagement von Industrieunternehmen als auch die Versicherungswirtschaft vor große Herausforderungen stellt. Die klassischen Versicherungskonzepte für Sachrisiken, basieren auf der Tatsache, dass der Großteil des Unternehmenswertes aus bilanzierbaren, materiellen Vermögenswerten besteht, also aus Fabriken, Immobilien und Maschinen. Im Jahr 1975 setzte sich der Gesamtmarktwert der im S&P 500 vertretenen Unternehmen zu 83 Prozent aus materiellen Gütern zusammen. Im Jahr 2015 verringerte sich dieser Anteil drastisch auf 13 Prozent. Das bedeutet, der Wert eines Unternehmens setzt sich heutzutage überwiegend aus immateriellen Vermögenswerten wie geistiges Eigentum, Software und Daten zusammen und somit stehen auch diese Werte zum größten Teil im Risiko. Dies führt aus Unternehmenssicht zu einer Verschiebung der Priorität des Risikomanagements. Daneben lässt die Globalisierung und Vernetzung der Wertschöpfungskette ein immer komplexeres Betriebsunterbrechungsrisiko entstehen. Technologi-

sche Innovationen bieten zwar die Möglichkeit zur Reduzierung des Risikos, indem durch Datenanalysen und Sensortechnologien die Schadeneintrittswahrscheinlichkeit reduziert wird. Daneben erschaffen sie jedoch neue Risiken und verändern die Risikolandschaft dramatisch. Die hohen Verluste in Milliardenhöhe durch die Cyberattacken durch die Erpressungstrojaner „Wanna Cry“ und „Not Petya“ zeigen, dass Cyberrisiken sich zunehmend zu einem existenzbedrohenden Risiko entwickeln (vgl. Swiss Re Institute 2017, S. 2 ff.).

Obwohl die immateriellen Vermögenswerte überwiegend im Risiko stehen, herrscht eine große Deckungslücke in diesem Bereich. Während rund 59 Prozent der Sachwerte versichert sind, liegt der Anteil der versicherten immateriellen Vermögensgegenstände bei gerade mal 13 Prozent. Potenzielle Höchstschadenszenarien der immateriellen Vermögenswerte liegen mit 979 Millionen US-Dollar deutlich über denen der materiellen Werte mit 770 Millionen US-Dollar. Diese Diskrepanz lässt vermuten, dass viele Industrieunternehmen das Risiko aus den sogenannten „Intangibles“ unterschätzen. Aufgrund der nicht angemessenen Bilanzierung solcher Assetklassen, werden die Risiken oft missverstanden. Um dieser Gefahr entgegen zu wirken, sollten die immateriellen Vermögenswerte zu einem zentralen Element im Risikomanagementprozess integriert werden (vgl. Fischer Hirs 2018).

Nicht jedes dieser neuen Risiken ist versicherbar, dennoch hat sich die Versicherungswirtschaft weiterentwickelt und neue Lösungskonzepte herausgearbeitet. Mittlerweile bieten nahezu alle Industriever sicherer eine Cyberversicherung an und die Nachfrage in Europa wächst kontinuierlich. Im Rahmen der Betriebsunterbrechung hat die Versicherungswirtschaft auf den Wandel der Digitalisierung und globalen Vernetzung der Wirtschaft reagiert, indem Ertragsausfälle auch ohne vorherigen Eintritt eines Sachschadens versichert werden können. Sogar für Reputationsrisiken gibt es vereinzelt Lösungen. Sollten traditionelle Versicherungskonzepte nicht ausreichend Schutz bieten, greifen Versicherer auf den alternativen Risikotransfer zurück. Hier werden durch Einbeziehung des Kapitalmarktes neue Kapazitäten geschaffen. Neben dem Anbieten von neuen Versicherungskonzepten zur Absicherung von immateriellen Vermögenswerten, spielen Serviceangebote gerade in dieser Klasse von Risiken eine besondere Rolle. Eine Reputationsanalyse kann beispielsweise im Vorfeld Imageschwachstellen aufzeigen und IT-forensische Unterstützung beschleunigt die Wiederkehr in den Normalbetrieb nach einem Hackerangriff. Hier kann die Versicherungswirtschaft auf ihre Erfahrungen und Netzwerke aus Experten zurückgreifen. Versicherungsunternehmen verstehen sich als Partner im Risikomanagementprozess, weshalb eine ganzheitliche Unterstützung im Vordergrund steht. Aus diesem Grund werden Leistungen aus Risikoeinschätzung, Schadenprävention oder Unterstützung im Krisenmanagement immer wichtiger (vgl. Fischer Hirs 2018).

5.3 Marktentwicklung aus Sicht der Unternehmen

Im vorherigen Abschnitt wurde die Risikolandschaft der Industrieunternehmen vorgestellt, näher erläutert und entsprechende Versicherungslösungen dargestellt. Die folgenden Abschnitte befassen sich mit der Entwicklung des Marktes aus verschiedenen Perspektiven. Als erstes erfolgt eine Analyse der Risiken aus Sicht der Unternehmen, indem die Veränderungen der größten Risiken im Zeitverlauf näher untersucht werden. Dazu werden Studien des Versicherers Allianz Global Corporate & Specialty (AGCS) und des Maklers Aon herangezogen und gegenübergestellt. In einem zweiten Schritt soll im Rahmen einer regionalen Analyse Unterschiede zwischen einzelnen Ländergruppen herausgearbeitet werden. Im Anschluss erfolgt eine Untersuchung der Marktentwicklung aus Sicht der Versicherungsunternehmen. Hier liegt der Fokus auf der Profitabilität des Marktes und auf dem Phänomen der sogenannten Deckungslücke.

Im Vorfeld gibt der folgende Abschnitt einen Überblick globaler Risiken, losgelöst von der Industrie und Versicherungswirtschaft. Diese werden durch das World Economic Forum in Zusammenarbeit mit Marsh & McLennan Companies sowie der Zurich Insurance Group in einem jährlich erscheinenden Bericht, dem Global Risk Report, ermittelt.

5.3.1 Übersicht und Entwicklung globaler Risiken

Das World Economic Forum veröffentlicht jährlich den Global Risk Report, welcher die Ergebnisse einer Umfrage zusammenfasst, in der rund 1000 Experten und Entscheidungsträger zur aktuellen Risikosituation befragt werden. In dem Bericht werden die größten globalen Risiken und Herausforderungen identifiziert und analysiert. Abb. 5.2 und 5.3 verdeutlichen die Entwicklungen der Risikowahrnehmung der letzten zehn Jahre im Zweijahresrhythmus. Während Abb. 5.2 die Entwicklung der fünf größten Risiken in Bezug auf die Eintrittswahrscheinlichkeit darstellt, zeigt Abb. 5.3 eine Rangliste der Risiken mit dem höchsten Schadenausmaß.

Wie in Abb. 5.2 und 5.3 zu sehen ist, hat sich das globale Risikoprofil in den letzten zehn Jahren deutlich verändert. Im Jahr 2010 prägten überwiegend makroökonomische Risiken die Risikowahrnehmung der befragten Experten. Hierzu zählen unter anderem Zusammenstürze der Kapital- und Finanzmärkte oder extreme Marktpreisschwankungen. Auch in den Jahren davor dominierte diese Risikoklasse die Rangliste des Berichts. In den folgenden zehn Jahren verschob sich die Risikowahrnehmung der Befragten zugunsten anderer Risikoklassen. So sorgen sich die Experten zunehmend um Themen aus den Bereichen Umwelt, Gesellschaft oder Technologie. Insbesondere die Umweltrisiken nehmen in den neueren Berichten eine besonders wichtige Stellung ein und dominieren somit die Ranglisten. Im Jahr 2020 stehen die obersten fünf Risiken mit der höchsten Eintrittswahrscheinlichkeit und drei von fünf Risiken mit dem größten Schadenausmaß im Zusammenhang mit dem Klima. Daneben spielen gesellschaftliche Risiken wie Wasser-

Top 5 Global Risks in Terms of Likelihood

	2010	2012	2014	2016	2018	2020
1st	Asset price collapse	Income disparity	Income disparity	Involuntary migration	Extreme weather	Extreme weather
2st	China economic slowdown	Fiscal imbalances	Extreme weather	Extreme weather	Natural catastrophes	Climate action failure
3st	Chronic disease	Greenhouse gas emissions	Unemployment	Climate action failure	Cyberattacks	Natural disasters
4st	Fiscal crises	Cyberattacks	Climate action failure	Interstate conflict	Data fraud or theft	Biodiversity loss
5st	Global governance gaps	Water crises	Cyberattacks	Natural catastrophes	Climate action failure	Human-made environmental disasters

█ Economic █ Environmental █ Geopolitical █ Societal █ Technological

Abb. 5.2 Top 5 globale Risiken mit der höchsten Eintrittswahrscheinlichkeit. (Quelle: eigene Darstellung in Anlehnung an The Global Risks Report 2020, S. 2)

Top 5 Global Risks in Terms of Impact

	2010	2012	2014	2016	2018	2020
1st	Asset price collapse	Financial failure	Fiscal crises	Climate action failure	Weapons of mass destruction	Climate action failure
2st	Deglobalization (developed)	Water crises	Climate action failure	Weapons of mass destruction	Extreme weather	Weapons of mass destruction
3st	Oil price spikes	Food crises	Water crises	Water crises	Natural disasters	Biodiversity loss
4st	Chronic disease	Fiscal imbalances	Unemployment	Involuntary migration	Climate action failure	Extreme weather
5st	Fiscal crises	Energy price volatility	Infrastructure breakdown	Energy price shock	Water crises	Water crises

█ Economic █ Environmental █ Geopolitical █ Societal █ Technological

Abb. 5.3 Top 5 globale Risiken mit dem höchstem Schadenausmaß. (Quelle: eigene Darstellung in Anlehnung an The Global Risks Report 2020, S. 2)

oder Lebensmittelkrisen, erhebliche Einkommensunterschiede und unfreiwillige Migration eine erhebliche Rolle. Außerdem ist eine zunehmende Entwicklung im Bereich der technologischen Risiken zu erkennen. Hierzu zählen beispielsweise Cyberangriffe oder ein Zusammenbruch der Infrastruktur (vgl. World Economic Forum et al. 2020, S. 6 ff.).

5.3.2 Entwicklung der größten Industrierisiken

Sowohl der jährlich erscheinende Allianz Risk Barometer der AGCS als auch die im Zwei-Jahrestakt publizierte Global Risk Management Survey von Aon versuchen die größten Risiken für Industrieunternehmen zu identifizieren, indem sie weltweit Risikoexperten aus verschiedenen Unternehmen befragen. In Tab. 5.2 sind die Ergebnisse der Studien der AGCS aus den Jahren 2015 bis 2020 zusammengefasst. Sie zeigt eine Rangliste der zehn größten Risiken für das Jahr 2020 und die Platzierung dieser Risiken in den vergangenen fünf Jahren.

Wie der Tab. 5.2 zu entnehmen ist, befinden sich unter den zehn größten Risiken viele der im ersten Abschnitt vorgestellten klassischen Risiken. Dennoch hat sich die Risikolandschaft in den vergangenen Jahren verändert, sodass neue Risiken in die Rangliste aufgenommen wurden. Hier zeigen sich Parallelen den Entwicklungen globaler Risiken aus dem Bericht des World Economic Forums. So schreiben auch die Experten aus der AGCS Studie Risiken aus Cybervorfällen, neuen Technologien oder dem Klimawandel ein immer höheres Gewicht zu. Diese neuen Arten von Risiken verdrängen teilweise die klassischen Risiken auf die hinteren Plätze.

Im Jahr 2020 überholte das Cyberrisiko erstmals das Betriebsunterbrechungsrisiko, welches jahrelang die Rangliste des Allianz Risk Barometers anführte. Entwicklungen durch die Digitalisierung sorgten bei den Unternehmen für eine immer größere Abhängigkeit von ihrer IT-Infrastruktur. Diese wachsende Abhängigkeit geht mit einem steigenden Gefährdungspotenzial einher, was sich wiederum in der Entwicklung der Risikowahrneh-

Tab. 5.2 Top 10 Risiken weltweit gemäß AGCS. (Quelle: AGCS 2015, 2016, 2017, 2018, 2019, 2020)

Risiko	2020	2019	2018	2017	2016	2015
Cybervorfälle	1	1	2	3	3	5
Betriebsunterbrechung	2	1	1	1	1	1
Rechtliche Veränderungen	3	4	5	5	5	4
Naturkatastrophen	4	3	3	4	4	2
Marktentwicklungen	5	5	4	2	2	7
Feuer	6	6	6	7	8	3
Klimawandel	7	8	10			
Reputationsrisiken	8	9	8	9	7	6
Neue Technologien	9	7	7	10		
Makroökonomische Veränderungen	10			6	6	

mung der Unternehmen widerspiegelt. Während das Cyberrisiko im Jahr 2013 noch auf Platz 15 eingestuft wurde, stieg es seither in der Rangliste kontinuierlich auf. Im Jahr 2014 erreichte dieses Risiko erstmals einen Platz in der Top 10 und im Jahr 2019 teilte es sich den ersten Platz mit dem Betriebsunterbrechungsrisiko. Die häufigsten Ursachen für Cybervorfälle sind Daten- oder Sicherheitslücken, Spionage, Hackerangriffe, Erpressungssoftwares oder Fehler durch die eigenen Mitarbeiter. Sowohl die Anzahl als auch die Schadenhöhe aus solchen Ereignissen stieg in der Vergangenheit rasant an. Dieser Trend wird sich in der Zukunft tendenziell fortsetzen. Daneben sehen sich die Unternehmen aber auch strengeren Datenschutzbestimmungen und Schadenersatzklagen konfrontiert. Ein Datendiebstahl, bei denen mehr als eine Million Datensätze betroffen sind, kostet heute im Durchschnitt 42 Millionen Dollar. Dies entspricht einem Anstieg von rund acht Prozent gegenüber dem Jahr 2018. Vorfälle bei denen mehr als 50 Millionen Datensätze gestohlen werden, kosten durchschnittlich 388 Millionen Dollar, was einer Steigerung von rund elf Prozent gegenüber dem Jahr 2018 entspricht (vgl. AGCS 2020, S. 11 ff.). Dieser wachsende Trend spiegelt sich auch in den Leistungen aus der Versicherungsbranche wider. Analysen der AGCS haben ergeben, dass der durchschnittliche versicherte Schaden aus dem Cyberrisiko im Jahr 2018 mittlerweile mehr als zwei Millionen Euro beträgt, während der durchschnittliche Schadenaufwand aus dem Risiko Feuer/Explosion bei rund 1,5 Millionen Euro liegt (vgl. AGCS 2019, S. 12).

Nachdem das Betriebsunterbrechungsrisiko seit sieben Jahren ununterbrochen die Rangliste anführte, wurde es im Jahr 2020 vom Cyberrisiko abgelöst und rutschte erstmalig auf Platz zwei. Dennoch bleibt es eines der größten Industrierisiken, welche sowohl die Unternehmen als auch die Versicherungsgesellschaften regelmäßig vor Herausforderungen stellt. Insbesondere die Vielzahl aller Eintrittsmöglichkeiten ist hier kritisch einzustufen. So kann eine Unterbrechung des Betriebes aufgrund klassischer Ereignisse, wie ein Brand der eigenen Produktionsanlage, entstehen. Daneben können jedoch auch externe Faktoren, wie Naturkatastrophen oder politische Ereignisse, die Lieferkette von Zulieferern hemmen und zum Stillstand in der Produktion führen. Es ist jedoch wichtig zu erwähnen, dass nicht alle dieser immer vielfältiger werdenden Unterbrechungsrisiken über eine klassische Betriebsunterbrechungsversicherung abgesichert werden können. Als aktuelles Beispiel sei hier die Protestbewegung der sogenannten „Gelbwesten“ in Frankreich zu nennen, welche dazu führte, dass Einzelhändler einen Verlust von rund einer Milliarde Euro erlitten (vgl. AGCS 2019, S. 8). Die meisten dieser Schäden dürften durch eine klassische Betriebsunterbrechungsversicherung nicht abgedeckt sein. Schadenanalysen haben ergeben, dass nahezu alle großen Sachschäden mittlerweile ein Betriebsunterbrechungselement aufweisen, welches in der Regel den Großteil des Verlustes ausmacht. Beispielsweise ist der Betriebsunterbrechungsschaden aus einem Brand oder einer Explosion rund 45 Prozent höher als der korrespondierende Sachschaden. Die am meisten genannten Auslöser für Betriebsunterbrechungen sind Feuer/Explosionen, Naturkatastrophen und der Ausfall von Maschinen. Diese Tatsachen spiegeln die vielfältigen Ursachen und die Relevanz des Risikos wider und machen deutlich, warum es seit mehreren Jahren die Rangliste des Allianz Risk Barometers anführte (vgl. AGCS 2020, S. 14 ff.).

Naturkatastrophen rangieren seit Beginn der AGCS Studie auf den ersten vier Rängen, was die Bedeutung dieses Risikos aus Unternehmenssicht widerspiegelt. Grund für diese Bewertung könnte in der Unberechenbarkeit und den gravierenden Folgen von Naturkatastrophen liegen. Im Jahr 2018 betrug der volkswirtschaftliche Schaden durch Naturkatastrophen nach Schätzung der Swiss Re rund 155 Milliarden US-Dollar. Der inflationsbeinigte durchschnittliche Schaden der letzten zehn Jahre beträgt 220 Milliarden US-Dollar. Der versicherte Schaden lag im Jahr 2018 bei rund 76 Milliarden US-Dollar und der versicherte Zehnjahresdurchschnittsschaden lag bei 63 Milliarden US-Dollar. Bedingt durch den Klimawandel wird sowohl die Schadenhäufigkeit als auch die Intensität solcher extremen Ereignisse ansteigen (vgl. Swiss Re Institute 2019, S. 3 f.).

Die Risiken aus Markt- sowie rechtlichen Veränderungen rangieren ebenfalls seit Jahren in der Top 10 Liste. Hierzu zählen Themen wie Sanktionen, Strafzölle, der Austritt Großbritanniens aus der Europäischen Union oder Eingriffe von Regierungen in das Geschäftsmodell der Unternehmen. Im Jahr 2019 wurden rund 1300 Handelshemmisse registriert und der Handelsstreit zwischen China und den USA ließ den US-amerikanischen Durchschnittszoll von 3,5 Prozent im Jahr 2017 auf acht Prozent ansteigen. Daneben war das Jahr 2019 von starken Marktvolatilitäten und Unsicherheiten aufgrund von Handelskonflikten und politischen Risiken geprägt, welche sich im Jahr 2020 voraussichtlich fortsetzen werden (vgl. AGCS 2020, S. 17 f.).

Das Feuerrisiko befindet sich im Jahr 2020 auf Platz 6 des Allianz Risk Barometers. In früheren Berichten wurde dieses Risiko noch deutlich höher eingestuft. In den Jahren 2013 bis 2015 platzierten die Experten das Risiko auf Platz 3. In den folgenden Jahren nahm das Gefährdungspotenzial laut Einschätzungen der Befragten ab, weshalb es in den folgenden Jahren im Mittelfeld rangiert. In der Vergangenheit konnte ein Rückgang von Feuerschäden für große Unternehmen festgestellt werden. Die wesentlichen Gründe hierfür liegen in verbesserten Schutzmaßnahmen sowie im zunehmenden Ausbau des Risikomanagements. Dennoch ist zu berücksichtigen, dass sich in einigen Branchen der Wert von Vermögensgegenständen pro Quadratmeter im vergangenen Jahrzehnt vervierfacht hat. Dementsprechend hat sich auch das Gefährdungspotenzial aus Brandereignissen signifikant erhöht. Dies wiederum erhöht das Risiko aus Unterbrechungsschäden, denn Feuer ist die häufigste Ursache für eine Betriebsunterbrechung. Analysen der AGCS ergaben, dass der durchschnittliche Schadenaufwand aus dem Feuerrisiko rund 1,5 Millionen Euro beträgt (vgl. AGCS 2020, S. 18).

Auch Reputationsrisiken befinden sich seit dem Jahr 2015 ununterbrochen unter den größten Risiken der AGCS Studie, allerdings rangieren sie zwischen den Plätzen 6 bis 9. Sie werden zwar weniger bedrohlich eingestuft als die zuvor genannten Risiken, dennoch sind der Ruf und die Marke eines Unternehmens wertvolle Vermögenswerte. Unternehmenskrisen sind ein kritischer Faktor für die Reputation eines Unternehmens und die Anzahl an Krisenszenarien ist vielfältig. Hinzu kommt die Tatsache, dass der Einfluss von sozialen Netzwerken in den vergangenen Jahren stark zugenommen hat. Die rasche Verbreitung von Nachrichten kann das Eintreten von Unternehmenskrisen fördern. Schätzungen zufolge verbreiten sich mehr als ein Viertel aller Reputationskrisen innerhalb einer

Stunde und zwei Dritteln innerhalb von 24 Stunden. Außerdem wird geschätzt, dass sich die Auswirkungen am Kapitalmarkt seit Einführung der sozialen Medien verdoppelt haben (vgl. AGCS 2020, S. 22). So ist im Jahr 2018 der Wert von Facebook aufgrund von Datenskandalen innerhalb kürzester Zeit um fast 40 Prozent gesunken (vgl. AGCS 2019, S. 21).

Die bisher genannten Risiken befinden sich seit vielen Jahren im Allianz Risk Barometer. In den letzten vier Jahren sind jedoch neue Risiken hinzugekommen. So werden die Gefahren durch neue Technologien und dem Klimawandel immer stärker eingeschätzt. Diese Einschätzung teilen auch die Befragten der Studie des World Economic Forums. Neue Technologien eröffnen zwar Möglichkeiten für neue Geschäftsmodelle und helfen dem Management bestimmte Risiken zu minimieren. Dennoch entstehen durch sie auch neue Risiken, aus denen unerwartete Folgen resultieren können. Der Einsatz von Sensor-technik ermöglicht das Sammeln erheblicher Mengen an Daten und verbessert so die Qualität der Risikobewertung. Gleichzeitig entsteht mit der Vernetzung von Maschinen und Fabriken ein erhöhtes Potenzial von Cyber-Kriminalität. Die größten Herausforderungen der nächsten fünf bis zehn Jahre sind Themen aus den Bereichen künstlicher Intelligenz, digitaler Plattformen, das sogenannte „Internet der Dinge“, autonomes Fahren und digitaler Assistenzsysteme. Nach Einschätzungen der Befragten besitzen sie das größte Risikopotenzial (vgl. AGCS 2020, S. 22 f.).

Der Klimawandel hat enorme volkswirtschaftliche, politische und soziale Auswirkungen und ist, wie der Bericht des World Economic Forum bestätigt, eine der größten Herausforderungen dieser Zeit. Ohne Gegenmaßnahmen werden sich Naturereignisse wie Stürme, Überschwemmungen oder Dürren häufen. Im Jahr 2018 wurde dieses Risiko in der AGCS Studie zum ersten Mal auf Platz 10 gelistet und im Jahr 2020 befindet es sich sogar auf Platz 7. Analysen ergaben, dass die Anzahl von wetterbedingten Verlusten sowie Flutschäden seit dem Jahr 1980 um den Faktor 3 bis 4 gestiegen ist. Nach Einschätzungen der Unternehmen ist die größte Gefahr die Zunahme von Sachschäden aufgrund einer

Tab. 5.3 Top 10 Risiken weltweit gemäß Aon. (Quelle: Aon plc 2019)

Risiko	2019	2017	2015	2013	2011	2009
Verlangsamtes Wirtschaftswachstum	1	2	2	1	1	1
Reputationsrisiken	2	1	1	4	4	6
Beschleunigte Änderungsraten von Marktfaktoren	3	38	34	-	-	-
Betriebsunterbrechung	4	8	7	7	5	3
Verstärkter Wettbewerb	5	3	4	3	3	4
Cyberangriffe	6	5	9	18	18	25
Rohstoffpreisrisiko	7	11	11	8	8	5
Liquiditätsrisiko	8	12	12	9	10	7
Innovationsversagen/Verfehlten von Kundenbedürfnissen	9	6	6	6	6	15
Rechtliche Veränderungen	10	4	3	2	2	2

steigenden Anzahl an extremen Naturereignissen. Der Klimawandel kann sich jedoch auch auf operationeller, strategischer oder regulatorischer Ebene bemerkbar machen (vgl. AGCS 2020, S. 20 ff.).

Neben der AGCS führt auch das Maklerunternehmen Aon in regelmäßigen Abständen eine Umfrage zu den größten Unternehmensrisiken durch und fasst die Ergebnisse in einem Bericht zusammen. Tab. 5.3 zeigt, wie auch bereits Tab. 5.2, die zehn größten Risiken aus dem Bericht 2019 und deren Platzierungen in den vergangenen Jahren.

Bei näherer Betrachtung der Aon Umfrage fällt auf, dass es viele Gemeinsamkeiten zwischen der Rangliste beider Studien gibt. In beiden Studien werden Risiken durch Betriebsunterbrechungen, Cybervorfällen, rechtlichen Veränderungen, Marktentwicklungen, Reputationsschäden und dem Fachkräftemangel in der Top 10 Rangliste erwähnt. Es bestehen jedoch deutliche Unterschiede in der Platzierung dieser Risiken. So wird das Betriebsunterbrechungsrisiko, welches in der AGCS Studie ununterbrochen auf Platz 1 rangiert, lediglich auf Platz 4 eingestuft. Die Folgen aus dem Reputationsverlust dagegen werden durch die befragten Teilnehmer deutlich höher eingeschätzt und befinden sich seit 2011 auf den obersten vier Rängen. Die Bedrohungen aus einem verlangsamten Wirtschaftswachstum, verstärktem Wettbewerb oder rechtlichen Veränderungen werden im Vergleich zur AGCS Studie ebenfalls höher eingestuft. Bei der Beurteilung der Entwicklungen von Cyberrisiken zeigen beide Studien einen ähnlichen Trend. Während sie in der Vergangenheit noch weniger bedrohlich beurteilt wurden, gewinnen sie in aktuelleren Studien zunehmend an Bedeutung. Risiken aus den Gefahren Feuer oder Naturkatastrophen wiederum, werden in der Aon Studie deutlich schwächer eingeschätzt. Im Allianz Risk Barometer finden beide Risiken regelmäßig einen Platz unter den größten Industrierisiken. Doch in der aktuellen Umfrage von Aon aus dem Jahr 2019 werden beide Risiken nicht genannt (vgl. Aon plc 2019, S. 21 ff.). Lediglich die Berichte aus den Jahren 2015 und 2009 erwähnen Risiken aus Sachschäden, welche durch Naturkatastrophen oder Brände verursacht werden (vgl. Aon plc 2015, S. 36).

Die unterschiedlichen Einschätzungen der Risiken zwischen den beiden Studien kommen insbesondere durch die Zusammensetzung der verschiedenen Teilnehmergruppen zustande. Die AGCS befragt in ihrer Umfrage sowohl ihre Kunden und Makler, als auch interne Risikomanager, Underwriter und Experten in der Schadenabwicklung (vgl. AGCS 2019, S. 3). Die Studie von Aon erfasst eine erweiterte Gruppe von Teilnehmern. Hier werden neben den Risikomanagern auch die CFOs und CEOs befragt (vgl. Aon plc 2019, S. 17 ff.). Risikomanager sorgen sich vorrangig um Risiken, die unmittelbar mit Versicherungslösungen in Verbindung stehen, weshalb solche Risiken vermehrt im Allianz Risk Barometer auftauchen. CEOs und CFOs dagegen sorgen sich vorrangig um Risiken, die unmittelbar in Verbindung mit der unternehmerischen Tätigkeit stehen. Aus diesem Grund finden sich Nennungen wie ein verlangsamtes Wirtschaftswachstum, Reputationsschäden oder verstärkter Wettbewerb auf den oberen Plätzen der Rangliste (vgl. Swiss Re Institute 2017, S. 10).

5.3.3 Regionale Unterschiede der größten Industrierisiken

Nachdem nun die größten Risiken weltweit und deren Entwicklung in den vergangenen Jahren analysiert wurde, beschäftigt sich der folgende Abschnitt mit einer regionalen Analyse. Hierbei wird zwischen den Regionen Amerika, Asien-Pazifik, Europa und Afrika & Naher Osten unterschieden. Die Regionen weisen zwar einige Gemeinsamkeiten auf, es sind jedoch auch signifikante Unterschiede festzustellen.

Amerika weist in Bezug auf die größten Risiken ein recht statisches Bild auf. Hier werden die Gefahren aus dem Cyber-, Betriebsunterbrechungs- und Naturkatastrophenrisiko am stärksten eingeschätzt (vgl. AGCS 2015–2020). Insbesondere Nordamerika war in den Jahren 2015 bis 2017 die am stärksten betroffene Region von Cyberangriffen mit 303 bekannten groß angelegten Angriffen (vgl. Aon plc 2019, S. 32). Jedes dieser Risiken hat ein hohes Verlustpotenzial mit kurz- und langfristigen Konsequenzen.

Unternehmen in der Region Asien Pazifik schätzen, ähnlich wie in Amerika, das Betriebsunterbrechungsrisiko und das Naturkatastrophenrisiko am größten ein. Daneben sorgen sich die Experten aber auch vor Marktveränderung, wie ein verstärkter Wettbewerb durch den Eintritt neuer agiler Unternehmen oder Marktschwankungen sowie Marktfaktuationen. Auch die Angst vor Cybervorfällen wächst zunehmend an (vgl. AGCS 2015–2020). Der hohe Stellenwert des Marktrisikos resultiert in Chinas wirtschaftlichem Aufstieg, welcher Unternehmen aus den etablierten Volkswirtschaften in dieser Region wie Japan, Korea oder Australien vor große Herausforderung stellt. Viele chinesische Unternehmen werden von der Regierung unterstützt, indem sie uneingeschränkten Zugang zu kostengünstigen Kapital erhalten (vgl. Aon plc 2019, S. 31).

Europa dagegen zeigt ein durchwachsenes Risikoprofil. Wie auch in anderen Regionen werden die Risiken aus Betriebsunterbrechungen und Cyberangriffen als größte Gefahr eingeschätzt. Auf den folgenden Rängen befinden sich Risiken aus Markt- oder rechtlichen Veränderungen. Die hohe Einstufung dieser Risiken ist vor Allem im Austritt Englands aus der Europäischen Union und den damit einhergehenden Unsicherheiten für Unternehmen begründet. Der sogenannte Brexit ist für Firmen, die ihren Sitz sowohl in der EU als auch in England haben, eine große regulatorische Belastung (vgl. AGCS 2015–2020). Hinzu kommen Faktoren wie der wachsende Populismus in Ländern wie Österreich, Schweiz, Italien und Ungarn oder die gewalttätige Gelbwesten-Bewegung aus Frankreich. Auch die Verlangsamung des Wirtschaftswachstums in Deutschland bereiten den Unternehmen große Sorgen (vgl. Aon plc 2019, S. 27).

Anders als in den oben genannten Regionen prägen in Afrika und im Nahen Osten andere Risiken die Risikolandschaft. An erster Stelle stehen Risiken aus Marktveränderungen und makroökonomischen Änderungen. Politische Risiken werden ausschließlich in diesen Ländern als schwerwiegende Risiken erwähnt und stehen somit in der Rangliste in den Top 3. Hierbei handelt sich überwiegend um Länder mit instabilen Regierungen, welche durch das Handeln von Extremisten beeinflusst werden. Dieser Umstand hat auch Einfluss auf potenzielle Investoren und macht Langzeitinvestitionen nur schwer kalkulierbar (vgl. AGCS 2015–2020). Die Angst vor einem wirtschaftlichen Abschwung in diesen

Regionen resultiert aus den bewaffneten Konflikten, Terrorismus und politischem Chaos, was die wirtschaftlichen Aktivitäten beeinträchtigt (vgl. Aon plc [2017](#), S. 21).

5.4 Marktentwicklung aus Sicht der Versicherungsunternehmen

Nachdem der vorherige Abschnitt sich mit den Marktentwicklungen aus Sicht der Industrieunternehmen befasst hat, sollen die nachfolgenden Ausführungen die Entwicklungen des Marktes aus Sicht der Versicherungsunternehmen näher durchleuchten. Der Fokus liegt auf der Profitabilität des Industriever sicherungsmarktes. Dabei soll die These, ob sich der Industriever sicherungsmarkt in einer Phase der Marktverhärtung befindet, analysiert werden. Im Anschluss folgen Erläuterungen zur sogenannten Deckungslücke. Die Deckungslücke ist der Unterschied zwischen dem entstandenen wirtschaftlichen und den versicherten Schäden.

5.4.1 Profitabilität des Marktes

Der Industriever sicherungsmarkt ist ein wettbewerbsintensiver Markt und insbesondere in der industriellen Sachversicherung kämpft die Versicherungswirtschaft gegen langjährige Verluste und erfolglose Prämiensteigerungen an. Grundsätzlich kann bei der Prämienkalkulation zwischen zwei Betrachtungsweisen unterschieden werden. Die Bildung einer kollektiven Gefahrengemeinschaft bildet den Grundgedanken der Versicherung und ist zweifelsohne notwendig, um Großrisiken abzusichern. Auf der anderen Seite kann eine Berücksichtigung der individuellen Risikosituation des Industrieunternehmens sinnvoll sein. Die große Herausforderung für die Versicherungswirtschaft liegt darin, den richtigen Mix aus diesen zwei Positionen zu finden (vgl. Marsh GmbH [2019](#), S. 2).

Die industrielle Sachversicherung ist seit Jahren für viele Versicherer aufgrund hoher Schadenbelastungen nicht profitable. Das Jahr 2017 sorgte durch eine Vielzahl von Naturkatastrophen, insbesondere den drei Stürmen Harvey, Irma und Maria für Rekordaufwendungen von rund 143 Milliarden Euro. Risiken aus dem Bereich Feuer dagegen weisen einen historischen Tiefstand auf. Dennoch reichen die positiven Erträge aus der Feuerversicherung nicht aus, um die Verluste durch Naturkatastrophen auszugleichen. Im Ergebnis weist die Sachversicherungsbranche eine Combined Ratio von rund 100 Prozent auf und ist somit nicht profitabel (vgl. Willis Towers Watson [2018](#), S. 16). Dennoch verhinderte der intensive Wettbewerb auf dem deutschen Industriever sicherungsmarkt branchenweite Prämienanpassungen (vgl. Marsh GmbH [2018](#), S. 3). Im Jahr 2018 verlief die Feuerversicherung für viele Anbieter durch eine hohe Schadenfrequenz von kleinen bis mittleren Schäden negativ. Viele Versicherer veranlassten daraufhin Prämienanpassungen, welche, sofern sie moderat ausfielen, mehrheitlich angenommen wurden. Einzelne Branchen wie die Petro-, Grundstoffchemie, Lebensmittelindustrie oder Textilverarbeitung stellen aufgrund ihrer Risikosituation eine besondere Herausforderung dar. In diesen Bereichen wur-

den teilweise erhebliche Prämienanpassungen durchgesetzt (vgl. Marsh GmbH 2019, S. 4 ff.).

Die allgemeine Haftpflichtversicherung läuft mit gesunden Combined Ratios seit mehreren Jahren recht positiv für die Versicherer und sorgt damit regelmäßig für Gewinne. Versicherungsnehmer können in Form von Prämienreduzierungen oder kostenlosen Deckungserweiterungen von dieser positiven Entwicklung profitieren. Für dieses Risiko ist ausreichend Kapazität vorhanden und die Prämienentwicklung für das Jahr 2019 ist recht stabil mit leicht sinkenden Tendenzen (vgl. Marsh GmbH, S. 5). Im Bereich der Rückrufrisiken sind dagegen andere Trends zu beobachten. Hier belasten hohe Schadenfrequenzen und -aufwendungen sowohl im Automotive als auch im Non-Automotive Bereich die Versicherer. So ist beispielsweise die Anzahl der Rückrufe von Fahrzeugen von 2011 bis 2015 stetig gestiegen. Diese Entwicklungen sorgen dafür, dass die Versicherer damit beginnen ihre Portfolien anzupassen. Insgesamt kann in der Haftpflichtversicherung zwar nicht von einer breiten Marktverhärtung gesprochen werden, dennoch lassen sich Marktverhärtungstendenzen erkennen (vgl. Willis Towers Watson 2018, S. 10).

Die Prämien im Bereich der Managerhaftpflichtversicherung (D&O-Versicherung) befinden sich auf einem relativ niedrigen Niveau. Kapazitäten werden vereinzelt verringert, was jedoch durch den Eintritt neuer Marktteilnehmer kompensiert werden kann, sodass in der Breite noch ausreichend Kapazität vorhanden ist (vgl. Willis Towers Watson 2018, S. 8). Prämienanpassungen sowie Einschränkungen in den Versicherungsbedingungen können nur vereinzelt durchgesetzt werden. Für USbörsennotierte Unternehmen verläuft die Entwicklung jedoch drastischer. Durch Sammelklagen und eine hohe Anzahl an Schadefällen reduzieren einzelne Versicherungsunternehmen ihre Kapazitäten deutlich und fordern Prämien erhöhungen (vgl. Marsh GmbH 2019, S. 7 f.). Nach Einschätzung von Martin Zschech, dem Head of Financial Lines bei der AGCS, liegt die Combined Ratio des Marktes deutlich über 100 Prozent. Seit einiger Zeit nimmt die Schadenanzahl steigende Tendenzen an, weshalb die Sparte keine Profitabilität aufweist. Aus diesem Grund wird sich das Preisgefüge in der D&O Versicherung in der Zukunft verändern (vgl. Reifenberger 2019, S. 72 ff.).

Die Warentransportversicherung war in den vergangenen Jahren wenig ertragreich. Im Jahr 2017 lag die Schaden-Kosten-Quote bei 99 Prozent und hat sich gegenüber dem Vorjahr (106 Prozent) leicht verbessert. Die Transportversicherungsunternehmen zeigen sich gegenüber dem Neugeschäft nur bedingt zeichnungsfreudig und versichern neue Risiken nur zu angemessenen Konditionen mit guten Combined Ratios (vgl. Willis Towers Watson 2018, S. 21). Dennoch kann der Markt in der Breite als käuferfreundlich beschrieben werden und eine branchenweite Marktverhärtung im Bereich der Warentransportversicherung bleibt aus.

Die technische Versicherung (Maschinen- und Montageversicherung) generierte im Jahr 2017 Beitragseinnahmen in Höhe von zwei Milliarden Euro, weist eine Combined Ratio von 90 Prozent auf und ist somit eine attraktive Sparte für Versicherungsunternehmen. Grundsätzlich befindet sich die technische Versicherung in einer weichen Marktphase und ist somit recht versicherungsnehmerfreundlich. Die Versicherer bieten ausrei-

chend Kapazitäten an und die Beitragsentwicklung bleibt stabil (vgl. Willis Towers Watson 2018, S. 18).

Die Prämien für Kreditversicherungen befinden sich auf einem niedrigen Niveau, da durch den hohen Wettbewerb Anpassungen nur schwer durchzusetzen sind. Bei der Entwicklung von Unternehmensinsolvenzen zeigen sich zwei gegenläufige Trends. Zum einen ist die Anzahl der Insolvenzen im Laufe der Jahre stetig gesunken. Dem steht jedoch die gestiegene Anzahl an Großinsolvenzen mit entsprechend hohen Schadensummen gegenüber (vgl. Willis Towers Watson 2018, S. 14). Dennoch ist die Schaden-Kosten-Quote branchenweit relativ gut und sorgt für ein profitables Geschäft. Für politische Risiken besteht am Markt eine große Auswahl an Anbietern mit entsprechender Auswahl an Deckungskonzepten. Für bestimmte Länder, die eine negative Entwicklung der politischen Lage andeuten, schränken Versicherer ihre Leistungen ein bzw. erhöhen die Prämiensätze (vgl. Marsh GmbH 2019, S. 14 ff.).

Zusammenfassend ist festzuhalten, dass sich der Industriever sicherungsmarkt in einzelnen Sparten auf der Schwelle zur Marktverhärtung befindet, in anderen Sparten hat er diese bereits überschritten. Insbesondere in den Bereichen der industriellen Sachversicherung, Transportversicherung und in Teilen der Haftpflichtversicherung sind zum Teil deutliche Prämiensteigerungen erkennbar. Dennoch sind für die meisten Risiken ausreichend Kapazitäten vorhanden und die Versicherer weisen ein relativ stabiles Zeichnungsverhalten auf.

5.4.2 Deckungslücke

Der Unterschied zwischen dem entstandenen wirtschaftlichen und dem versicherten Schaden wird als Deckungslücke bezeichnet. In den vergangenen 26 Jahren sind die wirtschaftlichen Schäden deutlich stärker angestiegen, als die versicherten Schäden und somit hat sich auch die Deckungslücke entsprechend vergrößert. Im Jahr 2017 betrug sie insgesamt rund 193 Milliarden US-Dollar weltweit. Bei einem korrespondierenden wirtschaftlichen

Tab. 5.4 Katastrophenschäden im Jahr 2017. (Quelle: Swiss Re Institute 2018, S. 7)

Region	Anzahl	Versicherte Schäden		Wirtschaftliche Schäden		Deckungslücke
		In Mrd. USD	In %	In Mrd. USD	In %	
Nordamerika	66	119,1	82,5	244,2	72,4	51,2
Lateinamerika/Karibik	19	5,1	3,5	31,6	9,4	83,9
Europa	46	12,0	8,3	23,7	7,0	49,4
Afrika	40	0,8	0,5	2,9	0,9	72,4
Asien	112	5,0	3,5	31,2	9,2	84,0
Ozeanien/Australien	5	2,1	1,4	3,3	1,0	36,4
Meer/Weltraum	13	0,3	0,2	0,3	0,1	0
Welt	301	144	100	337	100	57,3

Gesamtschaden von 337 Milliarden US-Dollar entspricht dies einer weltweiten Deckungslücke von 57,3 Prozent. Tab. 5.4 verdeutlicht die Problematik dieses Phänomens anhand von Katastrophenschäden im Jahr 2017, unterteilt nach einzelnen Regionen (vgl. Swiss Re Institute 2018, S. 6 ff.).

Das Phänomen der Deckungslücke ist kein Neues und wird von der Versicherungswirtschaft seit Jahrzehnten kommuniziert. Dabei sind große Unterschiede zwischen den einzelnen Regionen festzustellen. Typischerweise ist die Deckungslücke in den sogenannten Emerging Markets größer, da die Implementierung von Maßnahmen zur Minderung des Katastrophenrisikos nicht mit dem Wirtschaftswachstum des Landes mithalten kann (vgl. Swiss Re Institute 2019, S. 22). Die obige stehende Tabelle verdeutlicht jedoch, dass es sich nicht um ein Problem handelt, welches ausschließlich in den Emerging Markets vorzufinden ist, sondern um ein global beobachtbares Phänomen. Denn sogar in Ländern mit einer hohen Versicherungsdurchdringung, wie etwa Nordamerika, lag die Deckungslücke im Jahr 2017 bei rund 51 Prozent. Das entspricht einem nicht versicherten Schaden in Höhe von 125 Milliarden US-Dollar. In Europa ist ein ähnliches Bild vorzufinden, denn hier beträgt Deckungslücke rund 50 Prozent. Die Situation in den Regionen Afrika, Lateinamerika und Asien ist jedoch gravierender. In Afrika waren im Jahr 2017 rund 72 Prozent der entstandenen Schäden nicht versichert, in Lateinamerika und Asien sogar über 80 Prozent (vgl. Swiss Re Institute 2018, S. 7). Das Jahr 2017 war aufgrund von zahlreichen Naturkatastrophen, insbesondere der drei Stürme Harvey, Irma und Maria, ein außergewöhnlich schadenbelastetes Jahr, weshalb die Deckungslücke entsprechend hoch ausfiel. Aber auch im Jahr 2018 lag sie bei 85 Milliarden US-Dollar, was einen prozentualen Anteil von rund 50 Prozent ausmacht.

Eine Verringerung der Deckungslücke und Erhöhung der Versicherungsdurchdringung erzeugen erhebliche Vorteile für die globalen Volkswirtschaften, sowohl für Entwicklungs- als auch Industrieländer. So führt ein Anstieg der Versicherungsdurchdringung von einem Prozent, schätzungsweise zu einer Verringerung der nicht versicherten Schäden aus Naturkatastrophen um 13 Prozent (vgl. Artemis 2016). Munich-Re-Chef Joachim Wenning führte in der Frankfurter Allgemeinen Sonntagszeitung auf, dass die Kosten für einen Anstieg der Versicherungsdurchdringung erwiesenermaßen niedriger sind, als würden die Betroffenen ihre Schäden selbst tragen müssen (vgl. Mec 2018).

Ein Zeitvergleich macht deutlich, dass die wirtschaftlichen Schäden stärker gewachsen sind als die versicherten Schäden. Entsprechend ist auch die Deckungslücke in den vergangenen Jahren gestiegen. Der gleitende Zehnjahresdurchschnitt der versicherten Schäden ist in den letzten 27 Jahren um 4,7 Prozent gestiegen, während die wirtschaftlichen Schäden um fünf Prozent angestiegen sind (vgl. Swiss Re Institute 2019, S. 3 ff.). Um diesem Trend entgegenzuwirken, kann die Versicherungswirtschaft Aufklärungsarbeit leisten, um das mangelnde Risikobewusstsein der Unternehmen zu verbessern. Mit ganzheitlichen Risikoanalysen lassen sich die Risiken im Unternehmen aufdecken und die EINTRITTSWAHRSCHEINLICHKEIT für einen Schaden ermitteln und ggf. sogar reduzieren. Versicherungsunternehmen können hier mit Risk Consultant Maßnahmen unterstützend tätig werden. So hat die AGCS beispielsweise in Süddeutschland Empfehlungen für den Bau

von Hochwasserschutzmauern ausgesprochen. Durch die Errichtung dieser Mauern konnte die Versicherbarkeit der betroffenen hochwassergefährdeten Regionen wiederhergestellt werden. Neben den finanziellen Mitteln für Versicherungskonzepte sollten Industrieunternehmen also auch Präventionsmaßnahmen in die Kalkulierung ihres Budgets mit aufnehmen. Da sich Katastropheneignisse jedoch nicht verhindern lassen, besteht nicht nur Handlungsbedarf im präventiven Bereich, sondern auch nach dem Eintritt eines Schadens. So ist ein professionelles „Business Continuity Management“ ein wichtiges Werkzeug, um den Fortbestand des Unternehmens sicherzustellen. Im Kern handelt es sich hierbei um die Entwicklung von Strategien und Plänen, damit selbst in kritischen Situationen, die wirtschaftliche Existenz des Unternehmens gesichert ist. Auch hier kann die Versicherungswirtschaft die Industrie durch ihre gesammelten Erfahrungen und dem angeeigneten Wissen unterstützen (vgl. Berger 2018).

5.5 Fazit

Der Risikomanagementprozess umfasst die Identifizierung, Analyse, Bewertung und Steuerung von Risiken. Insbesondere die Steuerung kann mithilfe der Versicherungswirtschaft vollzogen werden. Im Laufe der Zeit haben sich bestimmte Risiken herausgebildet, die als klassische Risiken bezeichnet werden können. Dazu gehören Sachrisiken wie Feuer oder Naturkatastrophen, Ertragsrisiken, Personenrisiken oder auch Produktrisiken und Umweltrisiken. Für sie hat die Versicherungswirtschaft im Laufe der Zeit passgenaue Absicherungskonzepte entwickelt. So besteht heutzutage die Möglichkeit, die Gefahr nahezu aller Industrierisiken auf Versicherungsunternehmen zu übertragen.

Das Risikoprofil der Industrie ist nicht nur enorm vielfältig, sondern befindet sich zusätzlich stetig im Wandel, weshalb auch der Risikomanagementprozess entsprechende Anpassungen vornehmen muss. In den vergangenen Jahren prägten überwiegend Risiken aus Betriebsunterbrechungen, Naturkatastrophen, Haftungsansprüchen oder Marktveränderungen die Risikolandschaft. Doch die Digitalisierung macht die Industrie zunehmend abhängig von Informationstechniken, sodass die Gefahr aus Cyberrisiken oder neuen Technologien stetig ansteigt und andere Risiken verdrängen. Darüber hinaus verändern sich auch die Risikoprofile der klassischen Risiken. Die wachsende Vernetzung global tätiger Unternehmen erhöht das Risiko von Rückwirkungsschäden in der Betriebsunterbrechung drastisch. Der Klimawandel wird sowohl die Anzahl wie auch die Intensität von Naturkatastrophen ansteigen lassen.

Das Risikomanagement muss diese Entwicklung genau beobachten und bei Notwendigkeit entsprechend reagieren, indem es die Maßnahmen zur Risikosteuerung anpasst. Zusätzlich sind regionale Unterschiede zu beachten. Zwar herrschen global betrachtet viele Gemeinsamkeiten unter den größten Industrierisiken, doch auf regionaler Ebene sind signifikante Unterschiede festzustellen. So sind beispielsweise die Regionen Afrika und der nahe Osten durch makroökonomische Veränderungen und politischen Risiken geprägt,

während der Rest der Welt das Betriebsunterbrechung- und das Cyberrisiko stärker einschätzt.

Auch die Versicherungswirtschaft ist in der Pflicht auf den Wandel der Risikolandschaft zu reagieren, indem sie ihre Deckungskonzepte weiterentwickelt. In einigen Bereichen ist dies bereits geschehen. Mittlerweile bieten nahezu alle Industriever sicherer Deckungen gegen Cyberrisiken an und Betriebsunterbrechungen können auch teilweise ohne vorherigen Eintritt eines Sachschadens versichert werden. Außerdem agieren viele Versicherungsunternehmen als Partner im Risikomanagement und unterstützen nicht nur im Prozess der Risikosteuerung, sondern auch bei der Identifizierung, Analyse und Bewertung von Risiken. Durch langjährige Erfahrung und Zugriff auf Expertennetzwerke bringen sie viele Vorteile in den Risikomanagementprozess mit ein.

Versicherungsunternehmen stehen vor der Herausforderung der angemessenen Tarifierung und dem Zwiespalt zwischen dem Aufbau einer Gefahrengemeinschaft und der Berücksichtigung individueller Risikoprofile. In manchen Sparten wirkt sich die hohe Schadenbelastung negativ auf die Profitabilität aus, doch der intensive Wettbewerb verhindert zumeist, dass Versicherer ihre Bedingungen anpassen. Obwohl Sparten wie die industrielle Sachversicherung, die D&O Versicherung und in Teilen die Haftpflichtversicherung Combined Ratios von über 100 Prozent aufweisen, lässt eine Preissteigerung in der Breite noch auf sich warten. Somit befindet sich die gesamte Industriever sicherung auf der Schwelle zu einer Marktverhärtung.

Eine weitere Aufgabe der Assekuranz ist die Reduzierung der sogenannten Deckungslücke. Sie ist die Differenz zwischen dem entstandenen wirtschaftlichen Schaden und der versicherten Leistung. Dieses Problem wird zwar oft im Zusammenhang mit den Emerging Markets erwähnt, sollte jedoch als globales Problem betrachtet werden. In Regionen wie Afrika, Asien und Lateinamerika beträgt die Deckungslücke mehr als 70 Prozent und Nordamerika oder Europa weisen eine Deckungslücke von rund 50 Prozent auf. Die Versicherungswirtschaft ist hier in der Pflicht Aufklärungsarbeit zu leisten, indem sie als Partner im Risikomanagementprozess auftritt und das Risikobewusstsein der Unternehmen verbessert. Durch Bereitstellung von Analysetools und Risk Consultant Maßnahmen können sie den Risikomanagementprozess erheblich unterstützen. Die Verringerung der Deckungslücke hilft nicht nur einzelnen Industrieunternehmen, sondern führt zu einer Verbesserung der gesamten Wirtschaftsleistung aller Volkswirtschaften und somit dem globalen Wohlstand.

Literatur

- AGCS. (2015). Allianz risk barometer – Top business risks 2015. <https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2015.pdf>.
- AGCS. (2016). Allianz risk barometer – Top business risks 2016. <https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2016.pdf>.
- AGCS. (2017). Allianz risk barometer – Top business risks 2017. <https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2017.pdf>.

- AGCS. (2018). Allianz risk barometer – Top business risks for 2018. <https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2018.pdf>.
- AGCS. (2019). Allianz risk barometer – Top business risks for 2019. <https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf>.
- AGCS. (2020). Allianz risk barometer – Identifying the major business risks for 2020. <https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2020.pdf>.
- Aon plc. (2015). Global risk management survey. <https://www.lemoci.com/wp-content/uploads/2015/05/2015-Global-Risk-Management-Aon.pdf>.
- Aon plc. (2017). Global Risk Management Survey. <https://www.aon.com/2017-global-risk-management-survey/index.html>.
- Aon plc. (2019): Global Risk Management Survey. <https://www.aon.com/getmedia/6b9cacef-3ba1-4360-b470-dff66ce29d1a/aon-global-risk-management-survey-report-2019.pdf.aspx>.
- Artemis. (2016). Protection gap is the industry's „terrible failure“ and „great opportunity“. <https://www.artemis.bm/news/protection-gap-is-the-industrys-terrible-failure-and-great-opportunity/>. Zugegriffen am 30.04.2019.
- Berger, A. (2018). Nach dem Sturm, In *Herbert Frommes Versicherungsmonitor*. <https://versicherungsmonitor.de/2018/02/14/nach-dem-sturm/>. Zugegriffen am 14.02.2018.
- Brühwiler, B. (1994). *Internationale Industriever sicherung – Risk-Management, Unternehmensführung, Erfolgsstrategien*. Karlsruhe: VVW.
- Czeremuga, C. (2016). Elementare Gefahren für Unternehmen: Versicherungsschutz prüfen und bei Bedarf erweitern. *Die VersicherungsPraxis*, 7, 3–6.
- Federkeil, T. (2016). Sicherheit in unsicheren Zeiten: Erfassung politischer Risiken. *Die VersicherungsPraxis*, 11, 3–6.
- Fischer Hirs, C. (2018). Immaterielle Vermögensgegenstände: die offene Flanke, In *Herbert Frommes Versicherungsmonitor*. <https://versicherungsmonitor.de/2018/12/18/immaterielle-vermögenswerte-die-offene-flanke/>. Zugegriffen am 18.12.2018.
- GDV. (2019). Feuer! – die verkannte Gefahr. https://www.gdv.de/de/themen/positionen-magazin/feuer%2D%2D48738?fbclid=IwAR2T2J3Iy13LOG-U1s0SMG6s_f5jbDQ-L5IbOi-VG7rVm0TtbFliVBxedj1Y. Zugegriffen am 18.06.2019.
- Klinkhammer, G. (2017). Produkthaftung: Instruktionsfehler und Folgerungen für die Praxis. *Die VersicherungsPraxis*, 9, 3–7.
- Klinkhammer, G. (2018). Umweltschadenversicherung in der Praxis – Gesetze, Rechtsprechung und Bedingungen. *Die VersicherungsPraxis*, 1, 6–9.
- Marsh GmbH. (2018). Versicherungsmarktreport 2018 Deutschland. <https://www.marsh.com/de/de/insights/research-briefings/marsh-versicherungsmarktreport-deutschland-2018.html>. Zugegriffen am 06.05.2019.
- Marsh GmbH. (2019). Versicherungsmarktreport 2019 Deutschland. <https://www.marsh.com/de/de/insights/research-briefings/versicherungsmarktreport-2019-für-deutschland.html>. Zugegriffen am 06.05.2019.
- Mec, G. (2018). „Wir versichern auch Ihren Flug zum Mars“. In *Frankfurter Allgemeine Sonntagszeitung*, 04.02.2018, S. 23.
- Mikosch, C. (1991). *Industrie-Versicherungen – Ein Leitfaden für nationale und internationale Unternehmen*. Wiesbaden: Gabler.
- Reifenberger, S. (2019). D&O-Versicherung in der Klemme. In *Finance Magazin* (Mai/Juni 2019), S. 72–74.
- Swiss Re Institute. (2017). Sigma 5/2017 – Gewerbeversicherung: Erweiterung der Versicherbarkeit durch Innovation. <https://www.swissre.com/institute/research/sigma-research/sigma-2017-05.html>.

- Swiss Re Institute. (2018). sigma 1/2018 – Natur- und Man-made-Katastrophen im Jahr 2017: Ein Jahr der Rekordverluste. https://www.swissre.com/dam/jcr:bab49919-2c0f-4ed6-afc4-f7f7b954382c/sigma1_2018_de.pdf.
- Swiss Re Institute. (2019). sigma 2/2019 – Natural catastrophes and man-made disasters in 2018: „secondary“ perils on the frontline. https://www.swissre.com/dam/jcr:c37eb0e4-c0b9-4a9f-9954-3d0b-b4339bfd/sigma2_2019_en.pdf.
- Willis Towers Watson. (2018). Industriever sicherungen MARKTspot 2018. <https://www.towerswatson.com/assets/markt/spot.PDF>.
- Wittgen, B. (2017). Königsdisziplin Kreditversicherung: Wie internationale Unternehmen ihre Forderungen richtig managen. *Die VersicherungsPraxis*, 12, 5–8.
- World Economic Forum, Marsh & McLennan, & Zurich Insurance Group. (2020). The global risks report 2020. <https://www.weforum.org/reports/the-global-risks-report-2020>.

Daniel Aschoff begann seine berufliche Karriere als Redakteur der Münchner Abendzeitung. 2010 entschied er sich für einen Wechsel in die Versicherungsbranche und begann als Referent Vertriebskommunikation in der Allianz Beratungs- und Vertriebs-AG. 2012 wechselte er von dort zur Allianz Deutschland AG, wo er als Leiter Kunden- und Vertriebsmedien unter anderem für das preisgekrönte Kundenmagazins „1890“ verantwortlich war. 2015 übernahm die Rolle des Leiters Interne Kommunikation bei der Allianz Deutschland AG. 2017 folgte der Wechsel zur Allianz Global Corporate & Specialty, wo er seitdem die Position des Regional Head of Communications in der Region Central & Eastern Europe inne hat.

Julian Heitmann beendete im Jahr 2015 seine Ausbildung zum Kaufmann für Versicherungen und Finanzen bei der Debeka. Anschließend studierte er Versicherungswesen mit den Schwerpunkten Rechnungslegung von Versicherungsunternehmen, Steuerlehre, Sach- und Betriebsunterbrechungsversicherung am Institut für Versicherungswesen der Technischen Hochschule Köln. Im Anschluss absolvierte er dort auch das Masterstudium Risk & Insurance. Während des Studiums arbeitete er als Werkstudent bei DEMA Finanzdienstleistungen.



Emerging Risks

6

Neue Risiken und deren Anforderungen an das Risikomanagement

Jörg F. Henne und Leonard Wenzel

Zusammenfassung

In einem Zeitalter, das durch rasante Fortschritte in der technologischen und medizinischen Forschung geprägt ist, entstehen neue Risiken mit erheblicher Dynamik. Neue, schwer einschätzbare Risiken bezeichnet man mit dem Sammelbegriff „Emerging Risks“ (ER). Sie sind für die Gesellschaft und für Unternehmen insofern bedrohlich, als das Schadenpotenzial und der Charakter dieser Risiken entweder teilweise oder sogar gänzlich unbekannt sind. Somit bedarf es intensiver Identifizierungs- und Bewältigungsmaßnahmen für die Früherkennung sowie Charakterisierung solcher Risiken.

In diesem Beitrag werden die Definition und die Eigenschaften von ER näher erläutert, der Zusammenhang zum Risikomanagement illustriert sowie Beispiele aus der Praxis dargestellt. Der Fokus liegt dabei auf der Versicherungswirtschaft, da sich Versicherungsunternehmen in ihrer Funktion als Risikoträger unmittelbar mit diesen Risiken auseinandersetzen müssen. Da sich der englische Begriff inzwischen in der Versicherungsbranche etabliert hat, wird er auch in diesem Buch so beibehalten.

J. F. Henne (✉)

Gesamtverband der versicherungsnehmenden Wirtschaft e. V., Bonn, Deutschland
E-Mail: joerg.henne@gvw.de

L. Wenzel

TH Köln, Institut für Versicherungswesen, Köln, Deutschland
E-Mail: leonard.wenzel1@gmail.com

6.1 Einführung und Definition

Was bedeuten die beiden Begriffe „Emerging“ und „Risk“? Bei ersterem handelt es sich um ein Partizip Präsens, es beschreibt in grammatischem Sinne eine aktive Handlung und leitet sich von dem englischen Verb „to emerge“ ab. Dieses lässt sich unter anderem als „entstehen“, „erkennbar werden“ oder „in Erscheinung treten“ übersetzen. Mit diesem Wort werden folglich Vorgänge beschrieben, die sich aktuell in der Entstehung befinden und neuartig zum Vorschein kommen. Der Risikobegriff hingegen kann unterschiedlich definiert werden, da es keine einheitliche Definition gibt. Im Allgemeinen kann ein Risiko aber als eine potenzielle negative Abweichung von einem erwarteten Ergebnis beschrieben werden. Dabei ist es unerheblich, wie hoch das Schadenpotenzial ausfällt, solange es nachteilige Auswirkungen mit sich bringt. Das Risiko steht im Gegensatz zur Chance, mit der eine positive Abweichung vom Ergebnis bezeichnet wird.

Zusätzlich sollte der Risikobegriff von dem Begriff der Ungewissheit getrennt werden. Bei einem normalen Risiko sind die Alternativen sowie ihre Eintrittswahrscheinlichkeiten weitgehend bekannt, was bei ungewissen Sachverhalten nicht der Fall ist. ER sind genau zwischen diesen zwei Begriffen einzuordnen. Das Gefahrenpotenzial, die Alternativen sowie der Charakter sind unsicher, da sie durch ihre Neuartigkeit noch nicht ausreichend identifiziert werden können. Dennoch bezeichnet man sie als „Risks“, da sie sich gerade möglicherweise in dem Prozess befinden, sich zu einem gewöhnlichen Risiko zu entwickeln, bei welchem dann die genannten Kriterien mit hinreichender Sicherheit beschrieben werden könnten.

Da keine einheitliche Definition des Begriffs „Emerging Risk“ vorhanden ist, finden sich in der Literatur einige Unterschiede in der Begriffserklärung (vgl. Tab. 6.1).

Tab. 6.1 Definitionen in der Literatur von Emerging Risks

Quelle	Definition
Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)	„Neu auftretende Risiken (emerging risks) sind neu aufkommende oder sich wandelnde Risiken, die schwer zu quantifizieren sind und größere Auswirkungen auf das Unternehmen haben können.“ (Bundesanstalt für Finanzdienstleistungsaufsicht 2016, S. 16)
Munich Re	„(...) nach unserer Definition potenzielle Trends oder plötzlich eintretende Ereignisse, die sich durch ein hohes Maß an Unsicherheit in Bezug auf ihre Eintrittswahrscheinlichkeit, auf die zu erwartende Schadenhöhe und ihre möglichen Auswirkungen auf Munich Re auszeichnen.“ (Munich Re 2019, S. 66)
Swiss Re Institute	„(...) sich neu entwickelnde oder verändernde Risiken, deren mögliche Auswirkung und Tragweite noch nicht genügend berücksichtigt werden können.“ (Swiss Re Institute 2016a, S. 1)

Diese Definitionen weisen einige Ähnlichkeiten auf. So heißt es zum Beispiel in allen Definitionen, dass es sich einerseits um gänzlich neu auftretende Risiken handeln kann, andererseits aber auch um Risiken, die bereits vorhanden sind, sich allerdings in bestimmter Weise verändert haben. Außerdem sind die Auswirkungen weitestgehend unbekannt, was in der Definition von Munich Re durch Begriffe wie „Eintrittswahrscheinlichkeit“ und „zu erwartende Schadenhöhe“ nochmals verdeutlicht wird.

Im Allgemeinen können ER schließlich wie folgt definiert werden:

- Emerging Risks sind solche Risiken, die mit einer gewissen Neuartigkeit entweder plötzlich oder allmählich in Erscheinung treten und deren Auswirkungen aufgrund unzureichender Informationen noch nicht hinreichend einschätzbar sind.

6.2 Eigenschaften von Emerging Risks

Die Identifizierung von ER ist mit der Frage verbunden, ob man das jeweilige Risiko überhaupt als ein solches Risiko bezeichnen kann oder nicht. Demnach sind Kriterien erforderlich, anhand derer man ein Emerging Risk definieren kann. Wie bereits in der Einführung erwähnt, spielt die Ungewissheit im Zusammenhang mit ER eine entscheidende Rolle. Sie ist auch für Versicherungsunternehmen ein entscheidender Begriff, da eine Versicherung der finanziellen Absicherung eines ungewissen Schadeneignisses dient. Daher sollte diese Frage zunächst mit einem versicherungstechnischen Ansatz beantwortet werden.

Tab. 6.2 Kriterien der Versicherbarkeit. (Quelle: eigene Darstellung in Anlehnung an Farny 2006, S. 38 ff.)

Kriterium	Beschreibung
Legalität	Das abzusichernde Risiko darf gemäß §§ 134 und 138 Bürgerliches Gesetzbuch weder gegen das Gesetz noch gegen gute Sitten verstößen.
Eindeutigkeit	Es muss Klarheit über die versicherten Interessen, Gefahren und Schadensarten, den versicherten Zeitraum und Ort sowie die Höhe der Versicherungsleistungen bestehen.
Zufälligkeit	Die versicherten Schäden müssen unvorhersehbar und unbeeinflussbar sein. Es muss eine „notwendige Ungewissheit über Entstehung und/oder Zeitpunkt und/oder Größe des Schadens“ (Farny 2006, S. 38) bestehen.
Schätzbarkeit	Die Schadenhöhen und Eintrittswahrscheinlichkeiten müssen schätzbar sein.
Unabhängigkeit	Es sollte kein „kein systematischer Zusammenhang zwischen den Schadensrealisationen“ (Jäger 2009, S. 68) bestehen.
Größe	Die Höhe der erwarteten Versicherungsleistungen muss in einem angemessenen Verhältnis zur Risikotragfähigkeit des Versicherungsunternehmens stehen.

6.2.1 Versicherungstechnischer Ansatz

Es stellt sich die Frage, woran die besagte Ungewissheit gemessen werden kann. Sie steht in einem engen Zusammenhang zu der Versicherbarkeit von Risiken, da ein Risiko eher als nicht versicherbar gilt, wenn primär unsichere Informationen vorliegen.

In der Literatur finden sich hierzu feste Kriterien der Versicherbarkeit. Tab. 6.2 erläutert jedes Kriterium.

Mithilfe dieser Kriterien können somit ER im Hinblick auf ihre Versicherbarkeit beurteilt werden. Die Kriterien Legalität und Größe können dabei eher vernachlässigt werden. Erstens wird Legalität bei allen zu versichernden Risiken durch das Bürgerliche Gesetzbuch vorausgesetzt. Zweitens muss die Risikotragfähigkeit, womit „die Fähigkeit eines Versicherungsunternehmens, Verluste aus identifizierten Risiken zu absorbieren, ohne dass daraus eine Gefahr für die Existenz des Unternehmens resultiert“ (Rohlf 2018, S. 55) gemeint ist, für versicherbare Risiken ohnehin gegeben sein. Sollten hier Einschränkungen vorliegen, so ließe sie sich auch manuell erzeugen, wie zum Beispiel durch das Hinzufügen von individuellen Höchstentschädigungen, Selbstbehalten, Obliegenheiten, Deckungsausschlüssen und sonstigen vertraglichen Vereinbarungen.

Eindeutigkeit, Zufälligkeit, Schätzbarkeit und Unabhängigkeit sind hingegen die entscheidenden Faktoren, die ein Risiko versicherbar bzw. versicherbarer machen und an denen die Ungewissheit gemessen werden kann. Somit kann ein Risiko grob als Emerging Risk bezeichnet werden, wenn es ein auffallend hohes Maß an Unsicherheit in Bezug auf diese Kriterien aufweist.

Tab. 6.3 Unterschiede des Emerging Risks zum gewöhnlichen Risiko. (Quelle: eigene Darstellung in Anlehnung an Käslin 2008, S. 29 ff.; Jäger 2009, S. 75; Heidemann 2015, S. 13 f.; Schweizerischer Versicherungsverband 2017, S. 6)

Gewöhnliches Risiko	Emerging Risk
Leicht zu identifizieren und quantifizieren	Verdeckt und unbekannt, kaum einschätzbar
Kann in bestehende Risikomanagementprozesse eingegliedert werden	Kein regulärer Prozess möglich, da nicht genügend Informationen vorhanden sind
Risikoprofil ist bekannt bzw. ist statisch	Risikoprofil verändert sich kontinuierlich bzw. ist dynamisch
Vorhandensein von Statistiken, Schadenerfahrungen und Rechtsvorschriften	Keine historischen Erfahrungswerte vorhanden
Kausale Zusammenhänge zwischen Risikoquelle und Schadenursache bekannt	Kausale Zusammenhänge nur bedingt nachweisbar
Kann räumlich eingegrenzt werden	Global vorhanden
Kann auf bestimmte Wirtschaftszweige eingegrenzt werden	Ubiquitär

6.2.2 Vergleichsansatz

Neben der versicherungstechnischen Perspektive können ER aber auch durch andere Methoden von gewöhnlichen Risiken abgegrenzt werden. Der vorherige Ansatz beschränkt sich auf die Prüfung bestimmter Kriterien anhand eines Risikos und vernachlässigt dabei aber dessen individuellen Charakter. ER haben bestimmte Eigenschaften, mit denen sie sich von gewöhnlichen Risiken abgrenzen lassen. Tab. 6.3 stellt verschiedene Charakteristika dar, die eher auf ein gewöhnliches Risiko oder ein ER deuten und zieht in diesem Zuge einen Vergleich.

Durch diese Eigenschaften können ER von gewöhnlichen Risiken noch weiter differenziert werden. Ein entscheidender Unterschied liegt in der Eingliederung in den „üblichen Risikomanagementprozess“. Dies ist bei ER nicht uneingeschränkt möglich. Außerdem ist festzuhalten, dass nicht nur in der Beschreibung des Risikocharakters, sondern auch im Umfeld dieser Risiken eine große Unsicherheit liegt: Die Kausalitäten können nur unsicher beschrieben und die räumliche und wirtschaftliche Auswirkung nur schwer bestimmt werden.

6.2.3 Varianten der Neuartigkeit

Bei der Kategorisierung von ER spielt die Neuartigkeit eine entscheidende Rolle. Es gilt dementsprechend zu klären, welche genaue Bedeutung der Begriff in diesem Kontext hat, denn als alleinstehender Begriff ist dieser sehr weit. Zur Eingrenzung gibt es verschiedene Ansätze:

Erstens kann es sich bei ER um solche Risiken handeln, die zuvor vollständig unbekannt waren (plötzliche Neuartigkeit). Ein typisches Beispiel hierfür ist das Terrorrisiko, welches mit den Terroranschlägen vom 11. September 2001 unmittelbar von dem einen auf den anderen Tag gänzlich neue Dimensionen angenommen hat.

Zweitens können es auch schleichend auftretende ER sein, welche schrittweise bzw. allmählich in Erscheinung treten (schleichende Neuartigkeit). Typisch hierfür sind Cyber-risiken: Diese gewannen durch die Digitalisierung immer mehr an Bedeutung und wurden für die globale Wirtschaft zunehmend bedrohlicher.

Drittens spricht man ebenfalls von ER, wenn es sich um Risiken handelt, die zwar bereits bekannt sind, sich allerdings weiterentwickeln könnten. Diese Risiken sind demnach nicht gänzlich, sondern nur teilweise unbekannt (dynamische Neuartigkeit). Folglich ist festzuhalten, dass ER im Allgemeinen in drei verschiedenen Arten in Erscheinung treten können (vgl. Käslin 2008, S. 28).

Entscheidend ist aber auch die chronologische Entwicklung eines Risikos und welche Prozessschritte damit in Verbindung stehen. Alle Risiken durchlaufen nach ihrer erstmaligen Identifizierung einen Entwicklungsprozess. Sobald ein potenzielles Risiko erkannt wird, wird es sich zunächst in der Phase der Ungewissheit befinden. In dieser Phase kann es entweder als Emerging Risk oder als Phantomrisiko klassifiziert werden.

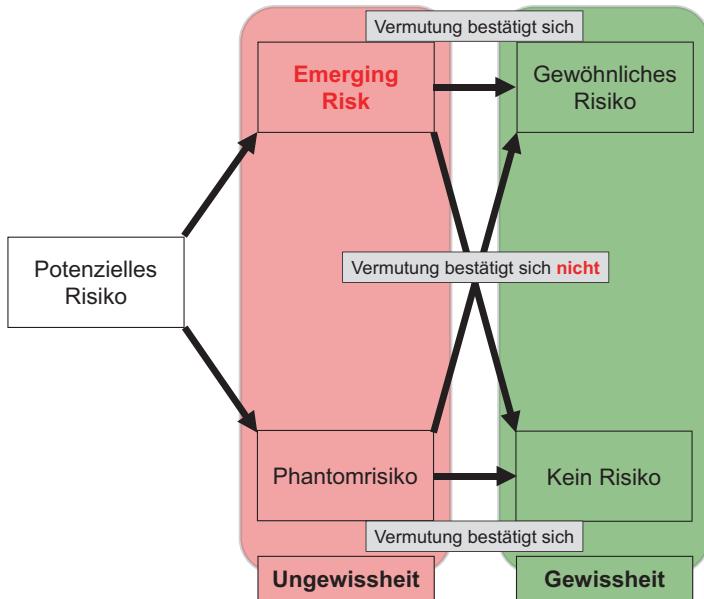


Abb. 6.1 Entwicklungsprozess eines Risikos. (Quelle: eigene Darstellung in Anlehnung an Käslin 2008, S. 25)

Der erste Begriff wird zumeist angewandt, wenn es bereits konkrete Indizien für das Vorhandensein eines bestimmten Risikos gibt, wobei der Charakter sowie die Auswirkungen des Risikos weiterhin unsicher sind. Überdies wird sich das Emerging Risk mit größter Wahrscheinlichkeit in Zukunft zu einem gewöhnlichen Risiko entwickeln.

Ist das Risiko aber lediglich mit groben Ängsten vor eventuellen Schäden verbunden und ist das Vorhandensein des Risikos nicht hinreichend aufgeklärt, so handelt es sich womöglich um ein Phantomrisiko, womit ein vermutetes Risiko gemeint ist, das in Wahrheit gar keines ist. Nach gewisser Zeit wird sich schließlich herausstellen, ob sich die einst aufgestellte Vermutung bestätigt hat oder nicht: In der Phase der Gewissheit wird dann dargelegt, ob die Klassifizierung als Emerging Risk oder als Phantomrisiko korrekt war (vgl. Käslin 2008, S. 25 ff.). Abb. 6.1 stellt den Prozess zusammenfassend dar.

Somit ist erkennbar, dass sich ER stets in einem dynamischen Umfeld befinden. Die Dauer eines solchen Prozesses kann dabei je nach Art des Risikos sehr unterschiedlich ausfallen. Demnach könnte sich der gesamte Zyklus einerseits über einen sehr kurzen Zeitraum, andererseits über mehrere Jahrzehnte erstrecken.

6.3 Bedeutung im Risikomanagement

Im klassischen Risikomanagementprozess haben sich bereits bestimmte Strukturen des Managements von Risiken etabliert. Diese sind nicht unbedingt immer auf ER anzuwenden, können aber auch für das Management von diesen Risiken hilfreich sein. Problematisch für das Managen von ER könnte sein, wenn Unternehmen diese in ihren unternehmenseigenen Prozessen gänzlich außer Betracht lassen, da eine Integration dieser Risiken die Komplexität erhöht und wenig Mehrwert für die Unternehmen bedeutet. Aus diesem Grunde stellt das Management von ER ein interessantes Forschungsgebiet im Risiko- und Schadenmanagement dar, da es mit unterschiedlichen Ansätzen betrachtet werden kann und im Status Quo noch einen hohen Entwicklungsbedarf beinhaltet. Im Folgenden werden zwei Ansätze für das Management von ER näher dargestellt.

6.3.1 Eingliederung in den Risikomanagementprozess

Einzelne Bestandteile des klassischen Risikomanagementprozesses sind durchaus von wichtiger Bedeutung für die Ermittlung von ER. Grundsätzlich finden sich die Hauptbestandteile des Risikomanagementprozesses in der Identifizierung, Bewertung und Steuerung von Risiken (vgl. Rohlf 2018, S. 75). Diese Phasen können nach einer entsprechenden Vorbereitung, insbesondere mit der Festlegung der individuellen Risikostrategie durch die Unternehmensführung, angegangen werden. Da allerdings sowohl Charakter als auch Bedrohungspotenzial von ER nicht hinreichend bekannt und einschätzbar sind, können die letzteren Prozessschritte nur schwer in der Praxis angewandt werden. Eine Anwendung wäre hier nur mithilfe von Hypothesen bzw. unsicheren Aussagen über den Risikocharakter, insbesondere Eintrittswahrscheinlichkeit und Schadenpotenzial, denkbar.

Die erste Phase des Risikomanagementprozesses, die Risikoidentifizierung, ist für ER ein entscheidendes Element. Die Aufgabe dieser Phase ist einerseits die Aufdeckung sämtlicher Risiken inklusive der Erfassung aller zugehörigen Details, zumindest insoweit, als eine Risikobewertung vorgenommen werden kann. Andererseits befasst sie sich auch mit der Analyse von zukünftigen Bedrohungspotenzialen und versucht in diesem Zuge, Trendlandschaften zu entdecken und dadurch neuartige Risiken abzuleiten (vgl. Rohlf 2018, S. 95). Die Erforschung von ER behandelt genau diese Aspekte. Ohne eine gründliche Risikoidentifizierung können ER nicht erkannt werden und entwickeln ein sich zunehmend erhöhendes Gefährdungspotenzial für Unternehmen und die Wirtschaft als Ganzes.

In einem engen Zusammenhang zur Risikoidentifizierung steht ein Risikofrüherkennungssystem, welches fortlaufend parallel zum Risikomanagementprozess in Unternehmen ausgeführt wird. Es umfasst sämtliche Maßnahmen der Unternehmensführung, die der frühzeitigen Erkennung existenzgefährdender Entwicklungen dienen. Wie zuvor erläutert, findet sich die größte Schwierigkeit der Risikoidentifizierung in der reinen Erken-

nung von Risiken, insbesondere im Falle von ER. Daher ist die Unterstützung durch ein Risikofrüherkennungssystem für Unternehmen unerlässlich.

Daraus lässt sich schlussfolgern, dass ein zuverlässiges und etabliertes Frühwarnsystem als Schlüssel für die frühestmögliche Aufdeckung von ER fungiert. Bei der Bewältigung dieser Aufgabe hilft zusätzlich die Risikoidentifizierung als Phase des Risikomanagementprozesses.

6.3.2 Emerging-Risk-Management

Neben einer Eingliederung in das bestehende Risikomanagement in Unternehmen gibt es zudem die Möglichkeit, einen selbstständigen Prozess für ER einzurichten – das Emerging-Risk-Management. Diese Methode kann für Unternehmen besonders dann von Vorteil sein, wenn Anwendungen über die bestehenden Prozesse zu aufwendig wären oder sie nicht zufriedenstellende Ergebnisse liefern sollten. Es geht hierbei um die Entwicklung eines strategischen Früherkennungssystems, welches sich speziell mit ER beschäftigt und parallel zum allgemeinen Risikomanagement ausgeführt wird. Gegenteilig hierzu wäre ein integrales Risikomanagement, welches sämtliche Funktionen inklusive Früherkennungssysteme in einen Gesamtprozess bündeln würde (vgl. Mayr und Sierpinski 2009). Aufgrund der wachsenden Komplexität der heutigen Risikolandschaft wäre diese Methode allerdings definitiv von Nachteil.

Der maßgebliche Unterschied zur Methode des Eingliederns in den Risikomanagementprozess liegt in der Organisation des individuellen Risikomanagements: Bei der Integration in bestehende Prozesse werden bekannte Risiken und ER gleichermaßen in das Risikomanagement eingeschlossen – es wird dabei keine besondere Differenzierung vorgenommen. Im Gegensatz dazu trennt das Emerging-Risk-Management diese beiden Kategorien voneinander: Dessen Aufgabe konzentriert sich einerseits auf die frühzeitige Erkennung von neuartigen Risiken sowie andererseits auf die Bestimmung des Risikopotenzials für die Wirtschaft und Gesellschaft inklusive des Ergreifens präventiver Maßnahmen, die einen kontrollierten Umgang mit diesen Risiken ermöglichen sollen (vgl. Heidemann 2015, S. 199).

Daraus lässt sich schließen, dass auch bei dieser Methode die reine Erkennung neuer Risiken im Vordergrund steht. Darauf aufbauend sollte dann eine bestmögliche Einschätzung des Gefährdungspotenzials auf die Umwelt vorgenommen sowie Maßnahmen für die Eindämmung entwickelt werden. Eine erfolgreiche Durchführung aller Prozessschritte wäre ideal, ist aber in der Praxis aufgrund der vorhandenen Menge an Informationen sowie der Schwierigkeit der Informationsbeschaffung selten realisierbar.

In der Literatur ist stets ein ähnlicher Prozess für strategische Früherkennungssysteme erkennbar. Abb. 6.2 stellt den groben Aufbau eines solchen Systems für Unternehmen dar.

Der Prozess beginnt mit einer Analyse der Unternehmensumwelt. Wurden die relevanten Umweltbereiche erkannt und hinreichend analysiert bzw. eingegrenzt, findet eine Herleitung von Trendlandschaften statt. Dort werden die konkreten Zusammenhänge sowie

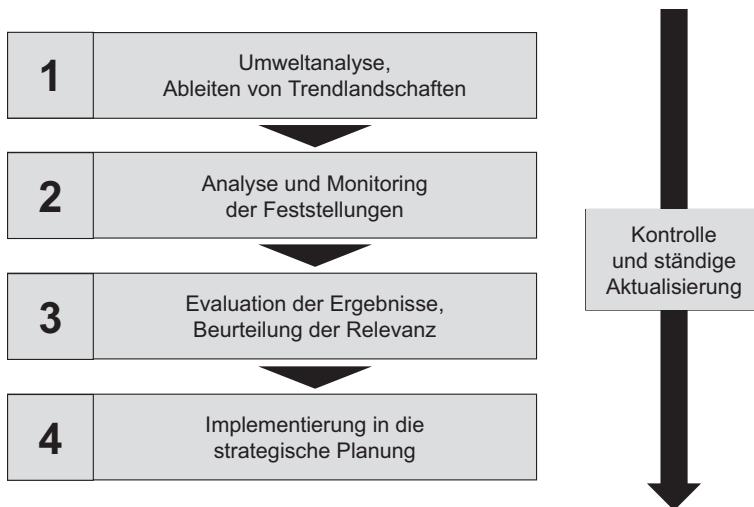


Abb. 6.2 Ablauf des Emerging-Risk-Managements. (Quelle: eigene Darstellung in Anlehnung an Heidemann 2015, S. 201 und Käslin 2008, S. 60)

Strukturen untersucht und bestmöglich festgestellt. Die Ergebnisse werden anschließend einer gründlichen Analyse sowie einem Monitoring unterzogen, das heißt, es „wird nach weiteren und ergänzenden Informationen gesucht, um bestehende Lücken zu schließen und Ungereimtheiten zu beseitigen“ (Käslin 2008, S. 63). Schließlich wird eine Evaluation einschließlich Bestimmung der Relevanz für das Unternehmen vorgenommen. Die Resultate werden daraufhin in die strategische Planung integriert. Parallel zum Gesamtprozess wird eine ständige Überwachung des Früherkennungssystems vorgenommen, da ein solches System aufgrund seiner zentralen Funktion einer ständigen Optimierung und Aktualisierung bedarf.

Im Ergebnis lässt sich festhalten, dass die Errichtung eines Emerging-Risk-Managements für betroffene Unternehmen einen hohen Mehrwert brächte. Gleichzeitig muss der zusätzliche Aufwand für ein solches System berücksichtigt und in ein Verhältnis zum Nutzen gesetzt werden. Dieses Verhältnis kann sehr unterschiedlich ausfallen. Somit lassen sich keine pauschalen Empfehlungen aussprechen. Die Möglichkeit des Aufbaus eines solchen Systems sollte Risikomanagern jedoch bekannt sein, um für ihr Unternehmen bewerten zu können, ob ein Einsatz sinnvoll wäre.

6.4 Beispiele aus der Praxis

Um ER rechtzeitig zu identifizieren und deren Potenzial zu bewerten, kann ein Blick in die Vergangenheit hilfreich sein. ER, welche sich in der Vergangenheit verwirklicht haben, wirken teilweise bis in die Gegenwart. Bei der Analyse ihrer Entstehung und Auswirkung können wichtige Erkenntnisse für den Umgang mit zukünftigen Risiken gewonnen wer-

den. Auch können Risiken, deren Potenzial erst in der Zukunft zu erkennen ist, schon heute grundsätzlich identifiziert werden und dadurch in die Risikomanagement Prozesse integriert werden.

6.4.1 Rückblick in die Vergangenheit

Um sich ein gutes Risikoverständnis von ER zu verschaffen, sollte zunächst die Vergangenheit betrachtet werden. Historische Risiken demonstrieren am besten, wie sich die Gefahren und das Schadenpotenzial in der Realität auswirken können. Die hier dargestellten Szenarien sind zwar auch heute noch als relevante Risiken anzusehen, sie hatten ihren Status als Emerging Risk im engeren Sinne jedoch bereits in der Vergangenheit besessen.

6.4.1.1 Asbest

In der wissenschaftlichen Forschung zu ER wird Asbest häufig als das vergangene Emerging Risk schlechthin dargestellt (so zum Beispiel Heidemann 2015, S. 13; Jäger 2009, S. 64 f.; Käslin 2008, S. 18), da es einerseits das mögliche Schadenausmaß und andererseits die Neuartigkeit bzw. die Falscheinschätzung, die bei solchen Risiken vorgenommen werden kann, anschaulich darlegt.

Alexander Jäger definiert Asbest in seiner Dissertation zu ER als „eine Sammelbezeichnung für Silicatminerale, [die] Materialeigenschaften wie extreme Hitze- und Säurebeständigkeit, große Festigkeit sowie sehr gute Wärmedämmung und Verarbeitungseigenschaften [aufweisen]“ (Jäger 2009, S. 64). Diese Eigenschaften waren für die industrielle Fertigung so sehr von Vorteil, dass sogar vom „Ruf eines Wunderwerkstoffes“ (Jäger 2009, S. 64) oder von einem „Material der tausend Möglichkeiten, da es wie keine andere Faser für viele technische Produkte optimale Eigenschaften besitzt“ (Schweizerischer Versicherungsverband 2017, S. 10), gesprochen wurde. Demzufolge kam Asbest im 19. und 20. Jahrhundert vielfältig in der Industrie zum Einsatz, da es in Kombination mit anderen Rohstoffen wie zum Beispiel Zement die Herstellung von sehr stabilen Materialien erlaubte. Typische Beispiele sind Stoffe für die Bauindustrie, Brems- und Kupplungsbeläge in der Automobilindustrie sowie Feuerhemmer im Brandschutz (vgl. WELT 2015; Stiftung Warentest 2017; Tacke 2017a, S. 1).

Schon im Jahre 1898 wurde die erste Warnung über Asbest als gesundheitsgefährdenden Stoff durch die britische Fabrikinspektorin Lucy Deane Streetfeild ausgesprochen (vgl. Gee und Greenberg 2001, S. 61; Horn 2011, S. 48). Ein Verbot wurde allerdings erst im späten 20. Jahrhundert ausgesprochen, da die Gefährdung bis dahin nicht wissenschaftlich nachgewiesen werden konnte, die gesundheitlichen Folgen als zu gering erachtet wurden und die Vorteile von Asbest überwogen. Diese lange Karenzzeit führte folglich zu einer weiträumigen Verbreitung asbestbedingter Krankheiten sowie zahlreichen Todesfällen (vgl. Gee und Greenberg 2001, S. 61; WELT 2015).

Die Gefahr bei Asbest liegt darin, dass die Faserpartikel leicht und unbemerkt eingeatmet werden können. Die faserigen Ablagerungen können daraufhin im Körper einen chro-

nischen Entzündungsprozess hervorrufen, der langfristig zu einer Versteifung des Lungen-gewebes führen kann. Dies verursacht wiederum Atemnot bei den Betroffenen, was das Hauptsymptom für die Lungenkrankheit Asbestose darstellt. Daneben können noch zahlreiche weitere Krankheiten verursacht werden, wie zum Beispiel Zwerchfell- und Lungenkrebs. Der Zeitraum zwischen erstmaliger Einatmung von Asbestfasern und Diagnose einer asbestbedingten Krankheit kann dabei mehrere Jahrzehnte betragen (vgl. Jend 2008; Schweizerischer Versicherungsverband 2017, S. 10; Tacke 2017a, S. 1).

Das Asbestrisiko ist heute längst nicht vollständig eliminiert. Dies zeigt sich darin, dass allein in den Vereinigten Staaten im Bereich der Schadenversicherung über die Jahre von 2013 bis 2017 noch ein durchschnittlicher jährlicher Schaden in Höhe von rund 1,9 Milliarden US-Dollar anfiel. Ferner bewertet das Unternehmen A.M. Best den kumulierten Gesamtschaden durch Asbest auf rund 100 Milliarden US-Dollar in den Vereinigten Staaten (vgl. A.M. Best Company 2018, S. 1).

Inzwischen sind die gesundheitlichen Folgen durch Asbestkontakt bekannt. Zudem ist die Verarbeitung und Verbreitung von Asbest in der Europäischen Union seit 2005 verboten. Laut UNO sind heute dennoch schätzungsweise ein Drittel der europäischen Bevölke- rung Asbest ausgesetzt (vgl. Swiss Re Institute 2018, S. 2). Der lange Zeitraum zwischen erstem Verdacht auf eine Gefährdung der Gesundheit und dem letztendlichen Verbot zeigt, welche weitreichenden Folgewirkungen ein Emerging Risk im Allgemeinen und die fal- sche Einschätzung eines solchen Risikos mit sich bringen kann.

6.4.1.2 Tabak

Ein weiteres Emerging Risk der Vergangenheit findet sich in der Tabakindustrie, insbeson- dere in den Vereinigten Staaten.

Das Desaster für die Branche begann im Jahr 2000, als eine Sammelklage von rund 8000 US-amerikanischen Familien dazu führte, dass die fünf größten Tabakkonzerne der Vereinigten Staaten zu einer Strafgeldzahlung in Höhe von 145 Milliarden US-Dollar verurteilt wurden. Der Grund für die Klage lag nahe: Die Unternehmen sollten offenbar die Verbraucher hinsichtlich der Gesundheitsrisiken vorsätzlich getäuscht haben, um ihren Umsatz auf einfache Weise zu steigern. 2003 annulierte ein Berufungsgericht in Florida diese Klage, da die Ausführung als Sammelklage angeblich nicht rechtens war, was der Oberste Gerichtshof wiederum im Jahre 2006 bestätigt hat (vgl. FAZ.NET 2003; Schlitt und Lindner 2006, S. 1). Allerdings ließen die Richter explizit zu, dass Einzelklagen wei- terhin gestellt werden könnten. So häuften sich in den darauffolgenden Jahren die Klagen von Angehörigen, in denen jeweils Straf- und Schmerzensgeld in Millionenhöhe auf die Tabakunternehmen zukam (vgl. Wernicke 2010). Im Jahre 2014 wurde der Hersteller R. J. Reynolds sogar zu einem Schmerzensgeld in Höhe von rund 23 Milliarden Dollar verurteilt, was im Rückblick jedoch einen deutlichen Ausreißer darstellt (vgl. Neue Zür- cher Zeitung 2014).

Diese Beispiele demonstrieren, dass Tabakunternehmen jederzeit und unerwartet von Schadenersatzklagen betroffen sein können. Zwar sollten die entsprechenden Unterneh-

men auf solche Klagen vorbereitet sein, allerdings bleibt es hier dennoch bei einem Risiko, das durch seinen plötzlichen und überraschenden Eintritt gekennzeichnet ist.

6.4.1.3 Cyber

Würde man Menschen auf der Straße auf ER ansprechen, würden vermutlich Cyberrisiken am häufigsten genannt. Der technologische Fortschritt sowie der Ausbau der weltweiten IT-Infrastruktur sind in den letzten Jahrzehnten so rasant vorangetrieben worden, dass das Risiko von Cyberangriffen für Unternehmen kontinuierlich wächst.

Heutzutage sind die typischen Eigenschaften von Cyberrisiken bekannt. Sie beinhalten „jegliche mit der Vernetzung und Nutzung des Internets und der Unangemessenheit oder des Versagens der IT-Systeme des Unternehmens im Zusammenhang stehende Gefahren, von Betriebsunterbrechungen durch sogenannte DoS-Attacken (Denial of Service, engl. für Dienstverweigerung) bis zum Datendiebstahl durch Hacker-Angriffe“ (Deutsche Aktuarvereinigung 2019, S. 17). Den Entwicklungsstatus als Emerging Risk hatten Cyberrisiken vor diesem Hintergrund bereits in der Vergangenheit.

Gleichzeitig stellen sie ein ideales Beispiel für die dynamische Neuartigkeit dar, die bei ER bestehen kann. Die Forschung in Bezug auf Cyberrisiken stellt einen kontinuierlichen Prozess dar, denn durch gegenwärtige Phänomene wie steigendes Datenaufkommen, stärkere Vernetzung aufgrund neuer Technologien wie zum Beispiel der neuen Mobilfunkgeneration 5G sowie eine wachsende Globalisierung können sich jederzeit neue Cyberrisiken entwickeln (vgl. Deutsche Aktuarvereinigung 2019, S. 18). Dieser Prozess wird auch in der Zukunft weiter fortschreiten. Demnach stellt diese Risikogruppe für Unternehmen ein großes Gefahrenpotenzial dar, da sich im Cyberbereich noch neue Risiken verbergen und sie hohe potenzielle Schäden bewirken könnten.

6.4.2 Die wichtigsten Emerging Risks von heute

Die globale Wirtschaft wird durch eine Vielzahl von ER kontinuierlich bedroht. Eine Aufstellung aller heute relevanten ER würde den Rahmen dieses Kapitels sprengen, zumal nie alle Risiken bekannt sein können. Aus diesem Grund wurde an dieser Stelle eine aussagekräftige Auswahl von heute relevanten ER in einer Risikomatrix zusammengefasst (vgl. Abb. 6.3). Dabei wird einerseits bewertet, wie dringend der Handlungsbedarf ist und andererseits wie das Schadenpotenzial zu beurteilen ist. Die Einordnung der ER in diese Matrix stellt eine Einschätzung der Autoren dieses Kapitels aus heutiger Sicht dar. Aufgrund der Komplexität und der geringen Menge an Informationen ist dies nur eine grobe Klassifizierung.

Diese Darstellung kann zwar nicht die gesamte Vielfalt der ER von heute abdecken, sie schafft aber einen Eindruck hinsichtlich der Risiken, die auf die Wirtschaft und Gesellschaft aktuell einwirken. Wie oben bereits erwähnt, werden nun drei Risiken näher erläutert, die die Eigenschaften und Auswirkungen eines ER anschaulich repräsentieren.

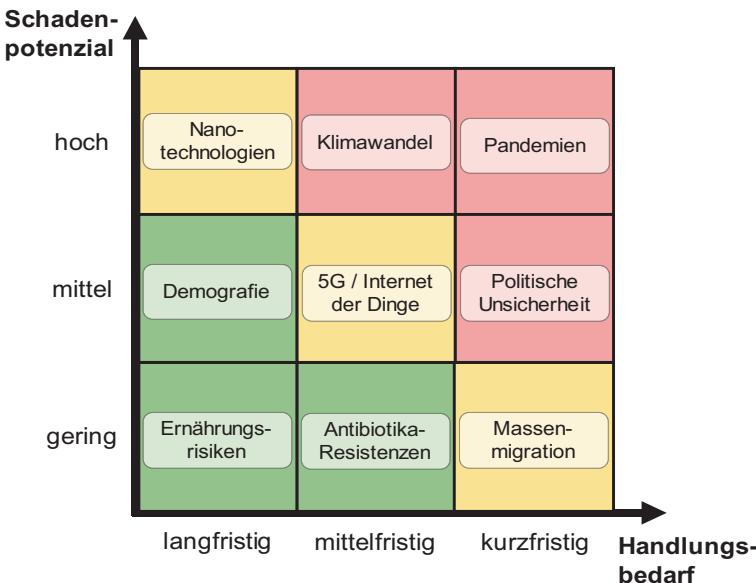


Abb. 6.3 Ausgewählte Emerging Risiken in einer Risikomatrix (Quelle: eigene Darstellung)

6.4.2.1 Nanotechnologien

Der Begriff der Nanotechnologien fungiert als Oberbegriff für industrielle Anwendungen, die mit Dimensionen im Nanometerbereich ausgeführt werden, was einem Milliardstel Meter entspricht (vgl. Jäger 2009, S. 77 f.; Tacke 2017b, S. 1). Sie bringen zwar eine Reihe von Vorteilen mit sich, stellen aber auch neue Risiken dar, die nur mit großer Unsicherheit beschrieben werden können. Allgemein liegt die Problematik bei Nanopartikeln darin, dass sie, sollten sie in freier Form vorliegen und nicht in ein Produkt integriert sein, möglicherweise in den menschlichen Körper gelangen und anschließend Krebskrankungen hervorrufen könnten, ähnlich wie Asbest (vgl. Schweizerischer Versicherungsverband 2018, S. 18).

Der maßgebliche Unterschied zu Asbest liegt im aktuellen Entwicklungsstatus: Die Risiken durch Nanotechnologien können aktuell nur mit großen Unsicherheiten beschrieben werden kann, wie es typisch bei einem Emerging Risk der Fall ist, während die Risiken durch Asbest inzwischen bekannt sind.

Die Versicherungsbranche ist von Nanotechnologien in mehreren Versicherungssparten betroffen. In der Lebens- und Krankenversicherung könnten sie zum Beispiel das Todesfall-, Berufsunfähigkeits-, Krankheits- sowie Invaliditätsrisiko sowohl positiv als auch negativ beeinflussen. Durch die neuen Methoden in der Krankheitsbekämpfung könnten ggf. Sterbe- und Krankheitswahrscheinlichkeiten reduziert werden. Gleichzeitig sind aber auch die Gesundheitsrisiken durch Nanotechnologien von Bedeutung, was wiederum eine gegenteilige Auswirkung mit steigenden Aufwendungen für Versicherungsfälle zur Folge hätte. Daneben sind Nanotechnologien auch für die Nicht-Lebensversicherung von Be-

deutung. Die Haftpflichtversicherung betreffend könnten nanoverarbeitende Industrien zum Beispiel von Verbrauchern bzw. entsprechenden Institutionen auf Schadenersatz verklagt werden. Ferner könnten bei Transportunfällen Umweltschäden entstehen (vgl. Deutsche Aktuarvereinigung 2019, S. 40 f.).

Diese kurze Beschreibung kann bei Weitem weder alle positiven noch alle negativen Auswirkungen abdecken, die durch Nanotechnologien verursacht werden. Es zeigt sich aber bereits ein sehr breites Spektrum an möglichen Schadenszenarien. Die Forschung befindet sich heute noch in einem frühen Entwicklungsstadium, weshalb Nanotechnologien ein Emerging Risk der Zukunft darstellen und die Gesellschaft noch längerfristig beschäftigen werden.

6.4.2.2 5G und das Internet der Dinge

5G, kurz für fünfte Generation, stellt den neuesten Standard in der Mobilfunktechnologie dar. Mit ihm sind unter anderem Datenübertragungsraten möglich, die die Raten der bisherigen Standards um ein Vielfaches übertreffen. Außerdem liefert 5G die Basis für das Internet der Dinge (Internet of Things), was eine Datenkommunikation zwischen künstlich intelligenten Geräten in Echtzeit bedeutet. Hierzu zählen zum Beispiel Maschinen, Roboter, Drohnen und autonom fahrende Autos, Bahnen sowie Schiffe. Die Deutsche Telekom spricht daher auch von einem „Kommunikationsstandard statt Mobilfunkstandard“ (Deutsche Telekom 2019).

Neue Technologien bergen stets neue Risiken. Neben der ohnehin größer werdenden Infrastruktur gibt es zum Beispiel Bedenken, dass die mit 5G verbundenen elektromagnetischen Felder gesundheitsschädlich sein könnten. Eindeutig nachweisbar ist bisher allerdings nur, dass sie eine thermische Wirkung haben (vgl. Tobien 2019). Sämtliche andere Folgen sind aktuell unklar. Weiterhin könnten auch diesbezügliche Cyberattacken neue Dimensionen annehmen, denn Geräte des Internet of Things haben üblicherweise geringe Sicherheitsfunktionen und funktionieren automatisiert (vgl. Swiss Re Institute 2019, S. 29). Der manuelle Einfluss durch den Menschen nimmt ab, was wiederum zu einer größeren Verwundbarkeit für Cyberangriffe führt. Ferner erlaubt die gestiegerte Leistung durch 5G einen schnelleren und umfangreicheren Datenzugriff und erhöht damit auch das Risiko des Datendiebstahls. Dazu sollte beachtet werden, dass der Einsatz des Internet of Things zwar menschliche Fehler eliminiert, Fehlfunktionen dieser Geräte jedoch zu immensen Schäden führen könnten (vgl. Deutsche Aktuarvereinigung 2019, S. 14).

Die genannten Schadenszenarien zeigen, dass unter anderem die Unternehmen, die an der Entwicklung der 5G-Technologie sowie der Herstellung von 5G-Modems und entsprechenden Geräten beteiligt sind, die Sicherheitsaspekte gleichermaßen wie die professionelle Entwicklung der Technologie berücksichtigen müssen. Werden diese Aspekte nicht ausreichend berücksichtigt, so könnte 5G extreme Schadenszenarien zur Folge haben.

6.4.2.3 Klimawandel

Mit dem Begriff Klimawandel ist im weiteren Sinne die globale Erwärmung, die insbesondere durch den Faktor Mensch und seine Aktivitäten verursacht wird, gemeint. Eine ein-

heitliche Definition gibt es nicht. Neben unklaren Definitionen sind allerdings die Kausalitäten bei diesem Risiko besonders kritisch zu betrachten, denn aktuell ist noch unklar, welche genauen Folgen allein auf den Klimawandel zurückzuführen sind. Es sind zwar erhebliche negative Auswirkungen erkennbar, allerdings ist die Bestimmung von Ursache und Zusammenhang meist mit großer Unsicherheit verbunden (vgl. Heidemann 2015, S. 205; Tagesschau 2017).

Es ist naheliegend, dass die Personenversicherungen durch den Klimawandel direkt betroffen sind. Die Gesundheitsrisiken können momentan nur grob eingeschätzt werden, allerdings ist eine Vermehrung extremer Wetterereignisse, unter anderem Dürren, Hitzewellen, Hochwasser und Stürme, sehr wahrscheinlich und damit die Auswirkungen auf den menschlichen Organismus. Die Hitzewelle in Frankreich im Jahre 2003 hat mögliche Auswirkungen bereits gezeigt: Sie führte zu rund 70.000 Todesfällen, mehrheitlich bei Personen höheren Alters. Durch den aktuell präsenten demografischen Wandel, also einer Erhöhung des Anteils älterer Menschen, führen solche Ereignisse in der Zukunft wahrscheinlich zu noch größeren Folgewirkungen. Schließlich stellt die auch zunehmende Wasserknappheit ein Langzeitsrisiko dar (vgl. Swiss Re Institute 2017, S. 31; Swiss Re Institute 2019, S. 44).

Auch die Sparten des Schaden- und Unfallbereichs sind durch den Klimawandel betroffen, insbesondere durch die zuvor genannten extremen Wetterereignisse, denn das Kumulschadenrisiko nimmt stark zu, was negative Auswirkungen auf Erstversicherer und Rückversicherer zur Folge hätte. Außerdem könnten Unternehmen durch neue Klimaschutzziele dazu aufgefordert sein, ihr Produktpotfolio grundlegend anzupassen, was hohe zusätzliche und unvorhersehbare Kosten verursachen könnte. Andererseits ist bei Verstößen gegen gesetzliche Auflagen mit entsprechenden Schadensersatzklagen zu rechnen, was ebenfalls ein zusätzliches Risiko darstellt. Dieser Aspekt ist besonders für die Berufs-, Umwelt- und Produkthaftpflichtversicherung relevant (vgl. Deutsche Aktuarvereinigung 2019, S. 33).

6.4.2.4 Pandemien

Der Begriff der Pandemie steht für die Ausbreitung einer Infektionskrankheit, der – im Gegensatz zur Epidemie – keine räumlichen Grenzen gesetzt sind. Die Risiken und Schäden, die durch eine Pandemie hervorgehen, sind weitreichend: Zum einen ist die Gesundheit der Menschen gefährdet, zum anderen wird die globale Wirtschaft vor erhebliche Herausforderungen gestellt.

Ein aktuelles Beispiel wird durch die COVID-19-Pandemie dargestellt, anhand der nachfolgend die Auswirkungen einer Pandemie exemplarisch gezeigt werden sollen. Die durch das Coronavirus SARS-CoV-2 ausgelöste Atemwegserkrankung hat ihren Ursprung in der chinesischen Metropole Wuhan, in der sie im Dezember 2019 erstmals identifiziert wurde und sich seitdem sukzessive ausbreitete, sodass sie am 11.03.2020 von der Weltgesundheitsorganisation WHO als Pandemie erklärt wurde (vgl. Page et al. 2020; World Health Organization 2020). Auf sämtlichen Kontinenten versetzte sie Wirtschaft und Gesellschaft vor nie gekannte Problemstellungen. So war zum Beispiel ein Drittel der gesamten

Weltbevölkerung von Ausgangsbeschränkungen betroffen (vgl. Thorwarth et al. 2020). Solche massiven Eingriffe in das öffentliche Leben können neben persönlichen und gesundheitlichen Belastungen auch große wirtschaftliche Schäden verursachen.

An dieser Stelle kann nur eine erste Idee der Folgen auf die Versicherungswirtschaft formuliert werden. Es ist naheliegend, dass die Ertragsausfallversicherung eine besonders betroffene Sparte sein wird. Üblicherweise greift der Versicherungsschutz dort jedoch nur, wenn der Ertragsausfall aus einem versicherten Sachschaden resultiert, wobei durch Viren grundsätzlich keine Sachschäden verursacht werden. Es könnten Schadensersatzansprüche aus Ertragsausfallversicherungen ohne vorausgegangenen Sachschaden bestehen. Hier ist jedoch zu prüfen, ob die Pandemie als versicherte Gefahr gilt. Weiter könnte die Haftpflichtversicherungssparte gefährdet sein: Hier könnten zum Beispiel Ansprüche aus der Verletzung der Fürsorgepflicht des Arbeitgebers, dem Ausbleiben von notwendigen Schutzmaßnahmen und Fehlentscheidungen im Rahmen von Betriebsschließungen erhoben werden. Auch die Personenversicherung werden erheblich belastet – so ergeben sich in der Krankenversicherung große finanzielle Einbrüche, da der Bedarf nach ambulanten und stationären Behandlungen höher sein wird als von den Versicherern kalkuliert wird. Weiter könnte die Lebensversicherung von einem erhöhten Sterblichkeitsrisiko betroffen sein. Selbstverständlich endet hier nicht die Liste von betroffenen Versicherungssparten und den möglichen Schadenszenarien. Daher kann zusammenfassend gesagt werden, dass die finanziellen Folgen einer Pandemie groß sein können, auch wenn das Eintreten einer Pandemie grundsätzlich ein selten auftretendes Phänomen ist (vgl. GVNW-Redaktion 2020, S. 32–36).

6.4.3 Fazit und Ausblick

Zusammenfassend lässt sich feststellen, dass das Forschungsgebiet der ER sowohl heute als auch in Zukunft eine hohe Relevanz haben wird. Es wurde gezeigt, dass sich der Charakter dieser Risiken wesentlich von gewöhnlichen Risiken unterscheidet und dass sie besondere Maßnahmen für das Risikomanagement erfordern. Die heutige Risikolandschaft von ER ist sehr global und multikausal, weshalb sich ein strukturiertes Management als höchst schwierig und umfangreich gestaltet. Unternehmen sollten dabei den Fokus auf die Früherkennung von ER setzen, um sich vor plötzlich eintretenden und potenziell sehr hohen Schadenszenarien weitestgehend zu schützen. Diese Früherkennung ist ein fortlaufender Prozess, den Unternehmen ständig aktiv behandeln und anpassen müssen.

Für die Versicherungswirtschaft sind ER nicht nur aufgrund der ungewissen Schadenausprägung besonders bedrohlich, sondern diese bergen auch eine außerordentlich hohe Gefahr für Kumulschäden. Die genannten Beispielrisiken haben gemein, dass sie zukünftig weitreichende Schäden verursachen könnten, sofern das Schadenausmaß nicht ausreichend eingedämmt wird. Die Absicherbarkeit von ER nimmt bei den Versicherungsnehmern einen hohen Stellenwert ein, da sie ihren bekannten Risiken bereits durch eigene, alternative Maßnahmen entgegenwirken.

Die Möglichkeit, unbekannte Risiken und ER auf Versicherer zu transferieren, ist für Versicherungsnehmer von hoher Bedeutung. Bekannte Risiken können Unternehmen durch gezieltes Risikomanagement begegnen. Somit sollten zukünftige Risiken nicht pauschal ausgeschlossen werden, sondern im gemeinsamen Dialog zwischen Versicherer und Versicherungsnehmer sinnvolle Möglichkeiten der Absicherung gefunden werden.

Effektives Risikomanagement darf sich nicht nur mit gegenwärtigen Risiken befassen. Die Identifizierung künftiger Risiken und das Ergreifen entsprechender präventiver Maßnahmen stellt für jedes Unternehmen eine zentrale Aufgabe dar, auch wenn sich solche Risiken möglicherweise erst bei künftigen Generationen entfalten werden. Vorausschauende Unternehmensführung beinhaltet, dass sich das Risikomanagement schon gegenwärtig mit ER auseinandersetzen sollte, damit auch solche Risiken bestmöglich eingedämmt werden können (vgl. Swiss Re Institute 2016b, S. 1). Auch deswegen ist es für Unternehmen erforderlich, zusätzlich ein Business Continuity Management (BCM) zu installieren, damit beim Eintritt eines Risikos möglichst schnell reagiert werden kann und Schäden minimiert oder abgewendet werden können.

Literatur

- A.M. Best Company. (2018). Best's market segment report – No slowdown in asbestos and environmental claims. <http://www3.ambest.com/bestweekpdfs/sr785211118561full.pdf>. Zugegriffen am 30.03.2020.
- Bundesanstalt für Finanzdienstleistungsaufsicht. (2016). Erläuterungen zu Leitlinien zum Governance-System. https://www.bafin.de/SharedDocs/Downloads/DE/Aufsichtsrecht/dl_erp_leitlinien_zu_governance_system_de_va.pdf?__blob=publicationFile&v=2. Zugegriffen am 04.06.2019.
- Deutsche Aktuarvereinigung. (2019). Ergebnisbericht des Ausschusses Enterprise Risk Management – Emerging Risks. [https://aktuar.de/unsere-themen/fachgrundsaetze-oeffentlich/2019-02-15_Ergebnisbericht_Emerging_Risks.pdf](https://aktuar.de/unsere-themen/fachgrundsaetze-oeffentlich/2019-02-15-Ergebnisbericht_Emerging_Risks.pdf). Zugegriffen am 07.07.2019.
- Deutsche Telekom. (2019). Was ist 5G? Grundwissen zum Netz der Zukunft. <https://www.telekom.com/de/konzern/details/was-ist-5g-grundwissen-zum-netz-der-zukunft-542352>. Zugegriffen am 21.07.2019.
- Farny, D. (2006). *Versicherungsbetriebslehre* (5. Aufl.). Karlsruhe: Versicherungswirtschaft.
- FAZ.NET. (2003). Tabakindustrie – Gericht verwirft Sammelklage gegen Tabakfirmen. <https://www.faz.net/aktuell/wirtschaft/tabakindustrie-gericht-verwirft-sammelklage-gegen-tabakfirmen-199114.html>. Zugegriffen am 27.07.2019.
- Gee, D., & Greenberg, M. (2001). Asbestos: From ‚magic‘ to malevolent mineral, In *Late lessons from early warnings: the precautionary principle 1896–2000*, S. 52–63. https://www.eea.europa.eu/publications/environmental_issue_report_2001_22/issue-22-part-05.pdf/view. Zugegriffen am 14.07.2019.
- GVNW-Redaktion. (2020). Praxistipp „Coronavirus“: Risiken und Versicherungsschutz, *Versicherungspraxis*, 3, 33–36.
- Heidemann, J. (2015). *Emerging Risks – Die neuen Gefahren und Chancen von morgen* (1. Aufl.). Münster/Westfalen: Wolters Kluwer.
- Horn, E. (2011). Die Zukunft der Dinge – Imaginationen von Unfall und Sicherheit. *Behemoth – A Journal on Civilisation*, 4, 2, Verlag Walter de Gruyter (heute: Bibliothek der Universität Freiburg). <https://ojs.ub.uni-freiburg.de/behemoth/article/download/762/688>. Zugegriffen am 13.07.2019.

- Jäger, A. (2009). *Risikobewertung und Risikomanagement von Emerging Risks in der Industriever sicherung – Einflussgrößen und Handlungsstrategien in der Versicherungsindustrie am Beispiel Nanotechnologien*. Stuttgart: Universität Stuttgart. https://elib.uni-stutt-gart.de/bitstream/11682/5527/1/Dissertation_NanoUndVersicherung_Jaeger_2009.pdf. Zugegriffen am 04.06.2019.
- Jend, H.-H. (2008). Fibrosierende Lungenparenchymkrankheiten, In *Einführung in die bildgebende Diagnostik der Lunge*. <http://www.mevis-research.de/~hhj/Lunge/Pneumokoniosen.html>. Zugegriffen am 14.07.2019.
- Käslin, B. (2008). *Systematische Früherkennung von Emerging Risks in der Versicherungswirtschaft*. St. Gallen: Universität St. Gallen.
- Mayr, R., Sierpinska, C. (2009). Integrales Risikomanagement mit Frühwarnsystem. In *Risk, Compliance & Audit, Ausgabe 6/2009*. <https://www.risknet.de/themen/risknews/integrales-risikomanagement-mit-fruehwarnsystem>. Zugegriffen am 13.07.2019.
- Munich Re. (2019). Risikobericht, In *Konzerngeschäftsbericht 2018*, S. 66–74. https://www.munichre.com/site/corporate/get/documents_E147443574/mr/assetpool.shared/Documents/0_Corporate_Website/Financial_Reports/2019/annual-report-2018/Risikobericht_2018.pdf. Zugegriffen am 12.06.2019.
- Neue Zürcher Zeitung. (2014). RJ Reynolds zu 23,6 Milliarden Schadenersatz verurteilt. <https://www.nzz.ch/wirtschaft/unternehmen/rj-reynolds-zu-236-milliarden-schadenersatz-verurteilt-1.18347205>. Zugegriffen am 27.07.2019.
- Page, J., et al. (2020). How it all started: China's early coronavirus missteps. *The Wall Street Journal*. <https://www.wsj.com/articles/how-it-all-started-chinas-early-coronavirus-missteps-11583508932>. Zugegriffen am 27.03.2020.
- Rohlfs, T. (2018). *Risikomanagement im Versicherungsunternehmen – Identifizierung, Bewertung, Steuerung*. Karlsruhe: Versicherungswirtschaft.
- Schlitt, P., & Lindner, R. (2006). Tabakindustrie – In die Zange genommen, In *FAZ.NET*. <https://www.faz.net/aktuell/wirtschaft/unternehmen/branchen-52-tabakindustrie-in-die-zange-genommen-1353944.html>. Zugegriffen am 27.07.2019.
- Schweizerischer Versicherungsverband. (2017). Emerging Risks – Eine Wertung der Arbeitsgruppe Emerging Risks der Fachkommission Haftpflicht des SVV, Release Nr. 6. https://www.svv.ch/sites/default/files/2017-11/emri_broschuere_release_6-2017-de_0.pdf. Zugegriffen am 04.06.2019.
- Schweizerischer Versicherungsverband. (2018). Emerging Risks – Eine Wertung der Arbeitsgruppe Emerging Risks der Fachkommission Haftpflicht des SVV, Release Nr. 7. https://www.svv.ch/sites/default/files/2018-11/SVV_Brosch%C3%BCCre_Emerging_Risks_2018_DE.pdf. Zugegriffen am 13.07.2019.
- Stiftung Warentest. (2017). Asbest – Die versteckte Gefahr. <https://www.test.de/Asbest-Die-versteckte-Gefahr-1269112-0/>. Zugegriffen am 14.07.2019.
- Swiss Re Institute. (2016a). Swiss Re SONAR – New emerging risks insights. <https://www.swissre.com/institute/research/sonar/swiss-re-sonar-new-emerging-risk-insights-2016.html>. Zugegriffen am 04.06.2019.
- Swiss Re Institute. (2016b). Medienmitteilung – Neuer SONAR-Bericht von Swiss Re untersucht die wichtigsten Emerging Risks für die Rück-/Versicherungswirtschaft und Gesellschaft. https://www.swissre.com/dam/jcr:ea5b83a0-01ba-437a-a8f5-2d26e5bf90a3/SwissRe SONAR_PR_DE.pdf. Zugegriffen am 04.06.2019.
- Swiss Re Institute. (2017). Swiss Re SONAR – New emerging risks insights. <https://www.swissre.com/institute/research/sonar/swiss-re-sonar-new-emerging-risks-insights-2017.html>. Zugegriffen am 13.07.2019.
- Swiss Re Institute. (2018). Swiss Re SONAR-Bericht 2018 beleuchtet Emerging Risks für Rück-/Versicherungswirtschaft und Gesellschaft. https://www.swissre.com/dam/jcr:20cf9bae-016f-4f35-ab6e-a69dae766b12/nr20180531_sonar_de.pdf. Zugegriffen am 13.07.2019.

- Swiss Re Institute. (2019). Swiss Re SONAR – New emerging risks insights. <https://www.swissre.com/institute/research/sonar/sonar2019.html>. Zugegriffen am 13.07.2019.
- Tacke, A. (2017a). Asbest. In *E+S Rück über Emerging Risks*. <https://www.es-rueck.de/1172302/asbest-2017.pdf>. Zugegriffen am 14.07.2019.
- Tacke, A. (2017b). Nanotechnologie. In *E+S Rück über Emerging Risks*. <https://www.es-rueck.de/1172478/nanotechnologie-2017.pdf>. Zugegriffen am 17.07.2019.
- Tagesschau. (2017). #kurzerklärt: Klimawandel. <https://www.tagesschau.de/multimedia/video/video-294087.html>. Zugegriffen am 24.07.2019.
- Thorwarth, K. et al.. (2020). Studie beweist: Ausgangssperren helfen bei Verringerung der Ausbreitung des Coronavirus. In *Frankfurter Rundschau*. <https://www.fr.de/panorama/studie-ausgangssperren-ausbreitung-coronavirus-deutlich-eingeschraenkt-zr-13603913.html>. Zugegriffen am 27.03.2020.
- Tobien, J. (2019). Neuer Mobilfunkstandard – Gefährdet 5G die Gesundheit?, In *Spiegel Online*. <https://www.spiegel.de/netzwelt/web/5g-gefaehrlich-was-experten-zum-thema-5g-und-gesundheit-sagen-a-1257267.html>. Zugegriffen am 21.07.2019.
- WELT. (2015). Asbest lauert dort, wo man ihn nie vermuten würde. <https://www.welt.de/gesundheit/article150200432/Asbest-lauert-dort-wo-man-ihn-nie-vermuten-wuerde.html>. Zugegriffen am 14.07.2019.
- Wernicke, C. (2010). Klagen gegen Tabakkonzerne – Die Folgen der Spätfolgen. In *Süddeutsche Zeitung*. <https://www.sueddeutsche.de/panorama/klagen-gegen-tabakkonzerne-die-folgen-der-spaetfolgen-1.487845>. Zugegriffen am 27.07.2019.
- World Health Organization. (2020). WHO Director-General's opening remarks at the media briefing on COVID-19 – 11 March 2020. <https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19%2D%2D-11-march-2020>. Zugegriffen am 27.03.2020.

Jörg F. Henne ist Geschäftsführer des Gesamtverbands der versicherungsnehmenden Wirtschaft – GVNW. Er begann seine berufliche Karriere als Referent für Versicherungen bei der Heidelberger Druckmaschinen AG. Ab 2004 war er Leiter Risk Management Insurance der EPCOS AG und verantwortlich für alle deutschen und die internationalen Konzernversicherungen, das ERM sowie das Claims Management. Ab 2005 war er Mitglied des Ausschusses beim DVS – Deutscher Versicherungs-Schutzverband und ab 2013 zudem Vorstandsmitglied, bevor er 2016 in die Geschäftsführung des Verbandes wechselte. Er studierte Rechtswissenschaften in Konstanz, Leeds und München und ist als Rechtsanwalt zugelassen. Jörg F. Henne ist verheiratet und hat zwei Töchter.

Leonard Wenzel studierte Versicherungswesen mit den Schwerpunkten Risikomanagement, Sachversicherung und Versicherungsmathematik am Institut für Versicherungswesen der Technischen Hochschule Köln und setzte dort seine Ausbildung mit dem Masterstudium Risk & Insurance fort. Seit Studienbeginn ist er bei der Deutschen Telekom Assekuranz tätig, bei der er heute als Data Scientist für das Belegschaftsgeschäft zuständig ist. Darüber hinaus unterstützt er in einer Nebentätigkeit die Forschungsstelle für finanzielles und aktuarisches Risikomanagement an der TH Köln.



Risiko- und Versicherungsmanagement

7

Detlef Hesse und Fabio Papa

Zusammenfassung

Gerade für international tätige Unternehmen stehen heute neben den klassischen Risiken (Feuer, Explosion etc.) zunehmend Risiken wie Betriebs- und Lieferkettenunterbrechungen, Naturkatastrophen, politische Risiken oder Cyberrisiken im Fokus.

Unternehmen benötigen heute nicht nur ein proaktives Risikomanagement, welches die vorhandenen Risiken erkennt und analysiert, sondern auch ein auf die einzelnen Risiken aufgebautes integriertes und transparentes Versicherungs- und Schadenmanagement.

Im Risikomanagement werden aus den Unternehmenszielen die einzelnen Formal- und Sachziele abgeleitet. Formal- und Sachziele variieren dabei in ihrer Gewichtung je nach Unternehmen. Formalziele wie Ökologieverträglichkeit (von Produkten) oder Nachhaltigkeit (Lieferkette und Produktion) gewinnen zunehmend an Bedeutung. Ein wesentliches Sachziel im Versicherungsmanagement ist die Versicherbarkeit von Risiken.

Risikomanager und Versicherungsmanager arbeiten in einem im Risikomanagement vollständig integrierten Versicherungsmanagement an gemeinsamen Lösungen. Hierzu gehört eine regelmäßige Bewertung der Risikostrategie und des Risikoappetits eines Unternehmens genauso wie die Optimierung der einzelnen Versicherungsprogramme. Zudem führt dies auch zu einer Minimierung der gesamten Risikokosten im Unternehmen.

D. Hesse (✉)

Electrolux Hausgeräte GmbH, Nürnberg, Deutschland

E-Mail: detlef.hesse@electrolux.com

F. Papa

TH Köln, Institut für Versicherungswesen, Köln, Deutschland

E-Mail: Fabio.Papa@outlook.de

Nicht alle Risiken sind jedoch versicherbar. In vielen Fällen können Risiken deshalb gegebenenfalls nur im Eigenbehalt getragen oder minimiert werden. Nicht zu unterschätzen sind auch vereinzelt auftretende Zielkonflikte zwischen Risiko- und Versicherungsmanagement, denn Unternehmen können in den einzelnen Unternehmensbereichen unterschiedliche Ziele, dargestellt durch sogenannte Key-Performance-Indicators (KPI), verfolgen.

7.1 Risiko- und Versicherungsstrategien eines Unternehmens

7.1.1 Three-Lines-of-Defence-Modell

Vor allem die Kontrollschwächen bei Banken haben in den letzten Jahren Bedenken hinsichtlich der Aufbau- und Ablauforganisation von Finanzunternehmen aufgeworfen. Das Three-Lines-of-Defence-Modell (TLoD) ist ein kohärentes und koordiniertes Kontroll- und Überwachungssystem, dessen Ziel es ist, die Verantwortlichkeiten und die Aufgaben der Bereiche und Funktionen eines Unternehmens klarzustellen (vgl. E&Y 2019, S. 1). Es ist notwendig die ohnehin knappen Risiko- und Kontrollressourcen zu koordinieren. Durch das TLoD kann vermieden werden, dass verschiedene Funktionen eines Unternehmens entweder zur selben Zeit dieselbe Einheit untersuchen und dadurch Ressourcen verschwendet werden oder dass Einheiten und Aktivitäten vergessen wurden geprüft zu werden, wodurch es zu einer Lücke kommt.

Die drei aufeinander aufbauenden Verteidigungslinien setzen sich zusammen aus Business Frontline (1. Verteidigungslinie), Risk und Compliance (2. Verteidigungslinie) und Auditors und Directors (3. Verteidigungslinie) (vgl. Welge und Eulerich 2014, S. 61).

In der ersten Verteidigungslinie entwerfen die Geschäftsbereiche Risikomanagement-kontrollen und setzen sie durch. Die operativen Einheiten stimmen die Kontrollmechanismen mit der Risikopolitik des Unternehmens ab und passen sie fortlaufend an. Die sogenannten Linienmanager sind für die Bewertung, Kontrolle und Minderung der Risiken innerhalb ihrer Einheit verantwortlich. Sie sind eine wesentliche Informationsquelle in Bezug auf Risiken im Unternehmen und eskalieren sie im Extremfall bis an den Vorstand. Im Regelfall berichten die Risikoverantwortlichen die wesentlichen Informationen in Form eines regelmäßigen Berichtes an das mittlere und obere Management (vgl. Anderson et al. 2009, Block 1, S. 32).

In der zweiten Verteidigungslinie unterstützen und überwachen verschiedene Governance-Organe, wie zum Beispiel das Risikomanagement, Controlling, der HR-Bereich oder Compliance, die operativen Einheiten. Es werden Rahmenbedingungen für die operativen Kontrollen und Kontrollmechanismen bestimmt und gesteuert. Sie überwachen nicht nur die jeweiligen Risikoberichte, sondern beeinflussen die Risikopolitik des Unternehmens maßgeblich.

In der dritten Verteidigungslinie werden die Restrisiken, die bislang noch nicht erfasst wurden, noch einmal durch eine unabhängige Instanz, welche maßgeblich durch die Interne Revision abgebildet wird, überprüft. Neben ihrer beratenden und überwachenden Rolle, stellt sie die Effektivität der ersten beiden Verteidigungslinien sicher, steigert bzw. schützt die Unternehmenswerte (vgl. Welge und Eulerich 2014, S. 62) und gewährleistet die Ordnungsmäßigkeit bei Überprüfung durch ein externes Wirtschaftsprüfungsunternehmen.

Der Aufgabenbereich der Internen Revision wird durch das TLoD-Modell erweitert und konkretisiert. Je nach Unternehmen bzw. Reifegrad, Ressourcen und Besetzung können die Verteidigungslinien im Modell variiert werden.

Auch ist das TLoD-Modell die Grundlage für die Risikopolitik des Unternehmens, die sich wiederum aus der jeweiligen Unternehmenspolitik ableitet. Die Risikopolitik wird in den meisten großen Unternehmen im sogenannten Riskmanagement Board (RM Board) definiert (der Name „Riskmanagement Board“ kann je nach Unternehmen variieren). Verstöße gegen die Risikopolitik des Unternehmens werden durch die Linienmanager an das RM Board hochskaliert und gemeinsam mit dem Unternehmensvorstand besprochen.

Eine Schwäche des TLoD-Modells ist, dass zwar wesentliche Risiken im Unternehmen erkannt und minimiert werden, es jedoch zu träge auf Veränderungen reagiert. Denn eine wesentliche Forderung an ein funktionierendes Risikomanagement ist, dass auf allen Entscheidungsebenen (strategisch, taktisch und operativ) ein proaktiver Ansatz implementiert wird (vgl. Anderson et al. 2009, Block 1, S. 37).

7.1.2 Formalziele und Sachziele des Risiko- und Versicherungsmanagements

Das Risikomanagement kann allgemein als ein Element verstanden werden, welches das Unternehmen darin unterstützt, seine Ziele zu erreichen (vgl. Hinterhuber 1998, S. 24 f.). Der Vorstand ist bei der Zielbestimmung des Risikomanagements unmittelbar beteiligt, indem er die Unternehmensziele definiert, aus welchen die Formal- und Sachzielen des Risikomanagements abgeleitet werden können (vgl. Huth 2004, S. 109). Bei deren Formulierung ist immer der Zieltyp, der zeitliche Bezug und das angestrebte Ausmaß zu bestimmen (vgl. Strohmeier 2007, S. 51). Auch ist die Beziehung zwischen den Zielen zu analysieren.

Man unterscheidet zwischen Formal- und Sachzielen. Dabei stehen Formalziele im direkten Bezug zu den Unternehmenszielen. Im Gegensatz zu den Sachzielen handelt es sich um monetäre Erfolgsziele, die sich auf ökonomische Größen beziehen oder Finanzziele zur Sicherung der Liquidität oder Existenz des Unternehmens.

Formalziele des Risikomanagements können unter anderem sein (vgl. Wolf und Runzheimer 2003, S. 35 f.; Hinterhuber 1998, S. 35 f.; Romeike und Finke 2003, S. 56 f.):

- Die Erreichung eines optimalen Risikoniveaus
- Die Existenzsicherung des Unternehmens
- Der künftige Unternehmenserfolg
- Die Minimierung der Risikokosten

Als Sachziele bezeichnet man solche Ziele, die sich aus den Formalzielen ableiten lassen und sich auf den jeweiligen Funktionsbereichen eines Unternehmens beziehen. Sie beziehen sich auf Objekte (zum Beispiel Güter, Anlagen) und Aktivitäten (zum Beispiel Dienstleistungen, Produktionsprozesse) des Unternehmens. Anders als Formalziele sind diese nicht monetär.

Sachziele des Risikomanagements können unter anderem sein (vgl. Götze et al. 2001, S. 73; Kaiser und Auer 2007, S. 161):

- Qualitätssicherung der Produktionsgüter
- Ökologieverträglichkeit
- Vermeidung von Störungen
- Sicherstellung der Produktion oder Lieferfähigkeit

Je nach Unternehmen variiert die Gewichtung der Ziele. Beispielsweise ist die Sicherstellung der Produktion und der Supply Chain in einem produzierenden Unternehmen eines der größten Formalziele. Eine Unterbrechung der Produktion führt zu einer Lieferkettenunterbrechung und verursacht in der Regel nicht nur zusätzliche Kosten mit nachfolgendem Umsatz- und Profitverlust, sondern kann auch letztendlich einen größeren immateriellen Schaden in Bezug auf Reputation und Marke mit sich bringen. Produzierende Unternehmen gewichten daher ihre Ziele anders als reine Handelsgesellschaften. Zunehmend gewinnen Sachziele wie die Ökologieverträglichkeit der Produkte und die Nachhaltigkeit in der Lieferkette und Produktion an Bedeutung. Unternehmen werden zukünftig bei ihren Lieferanten neben dem Kosten- und Qualitätsrating auch ein Nachhaltigkeitsrating durchführen.

Im Risikomanagement eines Unternehmens werden die wesentlichen Formal- und Sachziele erarbeitet. Das betriebliche Versicherungsmanagement ist Bestandteil des Risikomanagements. Ein wesentliches Sachziel im Versicherungsmanagement ist hierbei die Versicherbarkeit von Risiken. Aufgabe des Versicherungsmanagers ist für die einzelnen ermittelten Risiken entsprechenden Versicherungsschutz einzukaufen (Risikotransfer durch Versicherung). Nicht alle ermittelten Risiken sind im Rahmen des Risikotransfers versicherbar. Versicherungskapazitäten am Markt sind generell (beispielsweise bei Naturgefahren) begrenzt. Daher steht der Versicherungsmanager vor der Aufgabe, vorhandene Risiken auf ihre Versicherbarkeit hin zu analysieren:

- Die Versicherbarkeit generell zu prüfen und das Maß der Versicherbarkeit zu ermitteln (Versicherungsbedingungen, Ausschlüsse, Limite)

- Einen risikoadäquaten Preis zu verhandeln, zu denen die Risiken transferiert werden können (Prämienfindung)

Dabei können Zielkonflikte zwischen Risiko- und Versicherungsmanagement auftreten. Unternehmen können in den einzelnen Unternehmensbereichen unterschiedliche Ziele verfolgen, welche mit unterschiedlichen Key-Performance-Indicators (KPI) unterlegt sind. Beispielsweise wird ein Einkäufer von Produktionsteilen im Rahmen des Kostenratings auf eine möglichst optimale Rabattierung der Komponenten achten. Diese korreliert in der Regel mit der Abnahmemenge und wird dann erzielt, wenn die benötigten Zuliefererteile bei einem einzigen oder wenigen Lieferanten (Key Supplier) abgenommen werden. Die Konzentration auf wenige Lieferanten führt jedoch dazu, dass aus Sicht des Risikomanagements die „Kritikalität“ des Risikos zunimmt, da im Falle eines Lieferengpasses oder gar Ausfalls nicht unmittelbar auf einen alternativen Lieferanten ausgewichen werden kann. Für dieses Risiko müsste entsprechender Versicherungsschutz eingekauft werden, jedoch ist oft die Versicherbarkeit eines derartigen Risikos nicht in voller Höhe (Limitierung) gewährleistet, weswegen es zu Lücken im Versicherungsschatz kommen kann (Gap). Letztlich ist dann zu prüfen, ob ein Unternehmen die Differenz im Eigenbehalt tragen möchte (Risk Appetite). Hier ist es wiederum Aufgabe des Risikomanagers im Rahmen einer Risikoanalyse das potenzielle Risiko, aber auch das verbleibende Restrisiko aufzuzeigen. Zusammen mit dem Einkäufer werden verschiedene Lösungsansätze durchgespielt. Beispielsweise kann das Risiko auf mehrere Zulieferer verteilt werden. Das vorhandene Restrisiko wird so minimiert, die entstehenden Mehrkosten durch fehlende oder reduzierte Rabattierung wirken sich jedoch hier direkt auf den Profit des Unternehmens aus.

7.1.3 Risk Appetite und Risk Tolerance

Unter Risk Appetite (Risikoappetit) wird der Gesamtwert der Unternehmensressourcen verstanden, die der Vorstand einer Organisation bereit ist zu gefährden (vgl. Hopkin 2012, S. 209). Dabei wird kein fixes Konzept postuliert, sondern man spricht von „appetites“ für eine Vielzahl von Risiken. Diese sollten im Zusammenhang mit der Risk Management Capability (Risikomanagementfähigkeit) eines Unternehmens entwickelt werden, das wiederum von der Risk Capacity (Risikokapazität), dem maximalen Risiko, das ein Unternehmen eingehen darf, und der Risk Management Maturity (Risikomanagementreife) abhängt. Dabei ist es wichtig dem Risikoappetit auf strategischer, taktischer und operativer Ebene Rechnung zu tragen und in die Kontrollkultur der Organisation zu integrieren. Erst aus dem Zusammenspiel von Risiko und Kontrolle leitet sich der Risikoappetit eines Unternehmens ab (vgl. The Institute of Risk Management 2011, S. 8 ff.).

Die Risk Tolerance (Risikotoleranz) gibt den Wert des maximal akzeptablen Niveaus (Limit) an, dessen Überschreitung als alarmierendes Signal für ein Risiko betrachtet werden kann (zum Beispiel wenn eine Überschreitung zu einer Betriebsunterbrechung oder einer Verletzung von Gesundheitsvorschriften führt). Der Wert der Risikotoleranz wird durch das Management vorgegeben (vgl. Haksöz 2018, S. 162).

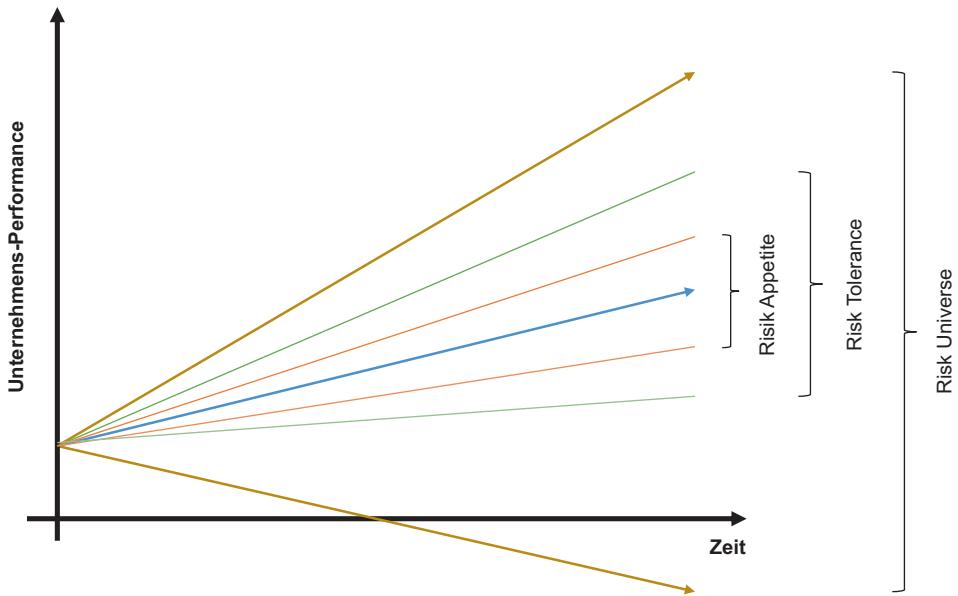


Abb. 7.1 Zusammenspiel von Risk Tolerance und Risk Appetite. (Quelle: eigene Darstellung)

Tab. 7.1 Schlüsselfaktoren für den Risikoappetit einer Organisation

Element	Beschreibung
Erwartungen der Aktionäre	Zielrisiko- und Ertragsprofil ausrichten mit: - Forderungen der Aktionäre; oder - die Leistungserwartungen des Vorstandes
Strategie	Kapazität und Toleranz für profitables Wachstum ausrichten
Finanzen	Gestaltung der Gesamtriskostufe durch Entscheidungen über die Bilanzstruktur (Leverage) und Risikotransfer (Absicherung oder Versicherung)
Geschäftsbetrieb	Angleichung der Akzeptanz und des tatsächlich eingegangenen Risikos der Geschäftsbereiche an das gewünschte Risikoprofil
Regulierungsstatus	Sicherstellung der geschäftlichen Aktivitäten im Einklang mit den Lizenz- und Gesetzesverpflichtungen

Quelle: eigene Darstellung in Anlehnung an Anderson et al. 2009, Block 3, S. 15

Die Performance eines Unternehmens hängt vom Zusammenspiel des Risikoappetits und Risikotoleranz ab (vgl. Abb. 7.1).

Die Grenzen der Risikobereitschaft sind entweder extern vorgegeben (zum Beispiel die Einhaltung der EU-DSGVO) oder werden intern durch das Management definiert (z.B. Verzicht auf Devisen- Spekulationsgeschäfte). Dieser Grenzwert ist geringer als das gesamte Risk Universe (Risikouniversum), da darin „unbekannte Risiken“ miteingeschlossen sind. In einem weniger ertragreichen Wirtschaftszeitraum eines Unternehmens wird der Vorstand möglicherweise einen größeren Verlust bei der Verfolgung der Unterneh-

mensziele tolerieren. Der Risikoappetit hingegen bewegt sich innerhalb der inneren Grenzen der Risikobereitschaft. Es liegt in der Verantwortung der Geschäftsführung das Risikomanagementsystem zu definieren und eine übereinstimmende Risikokultur im Unternehmen zu fördern. Für ein Unternehmen ist es daher unabdingbar ihre Risk Criteria (Risikokriterien) entlang ihres Risikoappetits zu bestimmen (Tab. 7.1).

Innerhalb dieser Risikokriterien werden Maßstäbe festgelegt, mit deren Hilfe die Risikoposition eines Unternehmens effektiv identifiziert, analysiert, bewertet und gesteuert werden kann (vgl. Anderson et al. 2009, Block 3, S. 14 f.).

Neben den Risikokriterien gibt es Risk Tolerance Categories (Risikotoleranzkategorien), nach denen der Risikoappetit eines Unternehmens ausgerichtet werden sollte. Man unterscheidet im Wesentlichen zwei Kategorien: Tolerierbare Risiken und nicht tolerierbare Risiken. Was tolerierbare Risiken sind, hängt vom jeweiligen Unternehmen ab (zum Beispiel von der Finanzkraft oder der Haltung der Geschäftsführung/Aufsichtsrates/Verwaltungsrates). Um zu bestimmen, wie hoch die Risiken sind, die ein Unternehmen tolerieren kann, werden diese in drei Klassen aufgeteilt:

- Upper: Unabhängig vom Nutzen nicht tolerierbare Risiken (zum Beispiel Zugunglück mit Todesfolge)
- Middle: Bedarf einer Kosten-Nutzen-Analyse zwischen Chance und Risiko (zum Beispiel Überreservierung von Sitzplätzen)
- Lower: Im Rahmen des Risikomanagements vernachlässigbare Risiken (Kleinere Vandalismusschäden)

Da es oftmals zunächst schwer ist, eine angemessene Balance zwischen Risikoappetit und Risikotoleranz zu finden, beginnt man meistens mit der Bestimmung der nicht tolerierbaren Risiken. Für gewöhnlich unterscheidet man qualitative und quantitative Aussagen. Bestimmt wird zunächst, welches Gesamtrisikolevel akzeptabel bzw. inakzeptabel ist, um somit eine Balance zwischen Risikoappetit und Risikotoleranz ermitteln (vgl. Anderson et al. 2009, Block 3, S. 15 ff.) (Tab. 7.2).

Tab. 7.2 Beispiele für quantitative und qualitative Aussagen

Quantitative Aussagen	Qualitative Aussagen
- Ein Verlust von Vermögenswerten über X Euro	- Die Reputation in einem Ausmaß beschädigen, sodass Stakeholders beginnen andere Organisationen zu frequentieren
- Ein Entstehen von nicht-budgetierten Verbindlichkeiten über X Euro	- Tod oder schwerwiegende Verletzung eines Mitarbeiters
- Unfähigkeit, über einen Zeitraum von mehr als fünf Tagen zu operieren	- Nichteinhaltung gesetzlicher Verpflichtungen

Quelle: eigene Darstellung in Anlehnung an Anderson et al. 2009, Block 3, S. 17

7.1.4 Auswirkung von Risiken und Unsicherheiten auf die Risikostrategie des Unternehmens

Die Zukunftsfähigkeit eines Unternehmens wird täglich durch zahlreiche Risiken bedroht. Risiken müssen beispielsweise vermieden werden, um die Zahlungsfähigkeit eines Unternehmens sicherzustellen, andere müssen hingegen getragen werden, um den eignen Gewinn zu maximieren (vgl. Anderson et al. 2009, Block 2, S. 5). Neben einer konsistenten Unternehmensstrategie, müssen Unternehmen daher auch eine dazu passende konsistente Risikostrategie entwickeln, deren Ziel es ist, die zukünftige Chancen-/Risiko-Politik des Unternehmens zu definieren und die Steuerung des unternehmerischen Gesamtrisikos und der Einzelrisiken zu ermöglichen (vgl. Schmitz und Wehrheim 2006, S. 95). Sie kann einem Unternehmen dabei helfen, Krisen zu vermeiden bzw. die Auswirkungen zu steuern, falls die Risiken sich bereits realisiert haben. Sie kann einem Unternehmen aber auch einen Wettbewerbsvorteil gegenüber Konkurrenten verschaffen.

Die Risikostrategie muss die Auswirkungen der Unternehmensstrategie auf die Risikosituation des Unternehmens umfassen. Daher leitet sie sich aus der individuellen Unternehmensstrategie ab und berücksichtigt das Risikoprofils des Unternehmens. Der Übergang zwischen Unternehmensstrategie und Risikostrategie ist oftmals fließend.

Um die eigene Risikoposition zu bestimmen, muss ein Unternehmen bestimmte Ereignisse und Umstände den zwei Dimensionen likelihood (Wahrscheinlichkeit) und consequence (Konsequenz) zuordnen. Unter Wahrscheinlichkeit versteht man die Häufigkeit, mit der ein Ereignis in einem bestimmten Zeitraum eintritt, wohingegen man unter Konsequenz den Grad der Auswirkung versteht, den ein Ereignis auf ein Unternehmen hat. Besonders bei Emerging Risks führt das Missing-Data-Problem dazu, dass die Wahrscheinlichkeit nur schwerlich geschätzt werden kann. Diese Ungewissheit kann auf vier grundsätzliche Unsicherheitsquellen zurückgeführt werden:

- Unvollständige Informationen
- Uneinigkeit zwischen Informationsquellen
- Sprachliche Ungenauigkeit zum Beispiel zwischen unterschiedlichen Kulturen
- Variabilität zum Beispiel bei Veränderung der Umstände oder Umgebung in der Physik oder Kultur

Oftmals werden Ungewissheit und Risiko synonym verwendet. Es ist jedoch unerlässlich zwischen ihnen zu differenzieren. Während Ungewissheit eine neutrale Tatsache ist, die einen Auf- und Abwärtstrend haben kann, ist das Risiko die negative Abweichung vom erwarteten Ausgang und folgt aus der Ungewissheit. Die Wahrscheinlichkeit und Auswirkung sind jedoch Dimensionen, die sich auf das Risiko eines Unternehmens beziehen. Mit ihrer Hilfe werden signifikante und nicht signifikante Risiken voneinander unterschieden. Ereignisse, die wahrscheinlich eintreten, jedoch keine oder nur geringe Auswirkungen haben, werden in der Regel als nicht signifikant eingestuft und dem Managementprozess überlassen. Im Risikomanagementprozess liegt der Fokus auf den Risiken, die wahr-

scheinlich oder unwahrscheinlich häufig eintreten, jedoch eine hohe, oftmals substanzelle Auswirkung auf das Unternehmen haben (vgl. Anderson et al. 2009, Block 2, S. 6 ff.). Häufig verwendet man Frameworks (zum Beispiel den zweidimensionalen Wahrscheinlichkeits-Konsequenz-Ansatz) zur Bestimmung der Signifikanz eines Risikos auf Basis beider Dimensionen. Dazu müssen zunächst alle Hauptrisiken identifiziert, wie auch alle Auswirkungen und Wahrscheinlichkeiten bestimmt werden.

Die Wahrscheinlichkeit, mit der ein Ereignis eintreten kann, ist jedoch oft schwierig zu bestimmen. Nicht nur das oben genannte Missing-Data-Problem erschwert die Bestimmung einer adäquaten Wahrscheinlichkeit, sondern auch die Tatsache, dass viele Risiken letztlich Ereignisse sind, die sich erst in der Zukunft realisieren. Die Wahrscheinlichkeit kann daher nicht gemessen, sondern nur geschätzt werden. Oft beeinflusst deshalb die subjektive Wahrnehmung und unbewusste Vorahnungen die Einschätzung des Risikos. Die Veranlagung, Informationen entlang seiner eigenen Erfahrungen zu interpretieren, wirkt sich auf die Reliabilität der geschätzten Werte aus.

Eine gründliche und fundierte Risikobewertung ist jedoch die Voraussetzung für ein wirksames Risikomanagementsystem. Eine fehlerhafte Einschätzung kann dazu führen, dass Risiken falsch priorisiert werden und sich die Konzentration auf die falschen Risiken verlagert. Wesentliche Risiken können nicht gesteuert werden und es kann im schlimmsten Fall zu einem Versagen des Risikomanagementprozesses kommen, der nicht nur mit dem Vertrauen an das Risikomanagement bricht, sondern zu einer existenziellen Bedrohung für das Unternehmen heranwachsen kann.

Die Erreichung der Projekt- und Geschäftsziele bedarf generell einer soliden Risiko-einschätzung, die frei von subjektiven Eindrücken ist. Daher ist es zwingend notwendig, sich des Problems bewusst zu werden und Verständnis für die Wichtigkeit einer adäquaten Risikoschätzung zu schaffen, als auch Maßnahme zu treffen, welche die Genauigkeit und Verbesserung der Risikobewertung gewährleisten. Die Anwendung verschiedener Techniken der Risikoschätzung kann dabei Abhilfe schaffen, um Befangenheitsquellen zu identifizieren und zu vermeiden. Auch muss sichergestellt werden, dass Maßnahmen zur nachhaltigen Verbesserung der Wahrscheinlichkeitsschätzung getroffen werden (vgl. Anderson et al. 2009, Block 2, S. 12).

7.2 Zusammenspiel von Risiko- und Versicherungsmanagement

7.2.1 Versicherbarkeit und Erarbeitung von Versicherungslösungen

Es wurde bereits ausgeführt, dass nicht alle Risiken versicherbar sind. In solchen Fällen können Risiken nur getragen oder minimiert werden. Ersteres geschieht im Sinne des bereits erwähnten Risk Appetite, bei dem aus strategischer Sicht Risiken getragen werden. Zur Minimierung von Risiken gehören zum Beispiel Maßnahmen zur Einschränkung der Geschäftstätigkeit (zum Beispiel territorial aufgrund geopolitischer Situation/Sanktionen) oder die Installation von Schadenverhütungssystemen.

In Fällen, in denen ein Risiko versicherbar ist, gibt es die Möglichkeit, eine neue Versicherung für das Risiko einzukaufen oder eine bestehende Versicherung risikoadäquat anzupassen. In beiden Fällen arbeiten Risiko- und Versicherungsmanager zusammen. Ausgangspunkt sollten immer die Ergebnisse der vorangegangen Risikoanalyse sein, welche dann die Grundlage für die nachfolgende Versicherungsanalyse bilden. Sofern firmeneigene Versicherungsunternehmen (Captives) existieren, sind zusätzlich deren Risikoprofil und die Neigung, bestimmte Risiken über die Captive zu versichern, zu berücksichtigen und ggf. mit dem Captive-Board abzustimmen.

7.2.2 Schadenmanagement als typische Schnittstelle für die Zusammenarbeit von Risikomanager und Versicherungsmanager

Wie schon oben erläutert, benötigen Unternehmen nicht nur ein vorausschauendes Risikomanagement, sondern auch ein auf die vorhandenen Risiken aufgebautes Versicherungs- und Schadenmanagement. Gerade im Schadenfall ist die Zusammenarbeit zwischen Risiko- und Versicherungsmanager unabdingbar. Aufgabe beider ist es zunächst, den betroffenen Unternehmensbereich bei der Schadensbewältigung, insbesondere bei der Schadensminimierung, zu unterstützen. Hier können Erfahrungen aus vergangenen Schadensfällen aber auch die des Versicherers wichtig sein. In einem zweiten Schritt sind letztendlich die Ergebnisse vorangegangener Risikoanalysen mit den Ergebnissen der Untersuchungen zum Schadenfall (durch Versicherer, Sachverständige aber auch eigene interne Untersuchungen) zusammenzuführen, (neu) zu bewerten sowie mit dem/den betroffenen Unternehmensbereich(en) durchzusprechen. In einem weiteren Schritt sind dann mögliche Auswirkungen auf die Risikopolitik und -strategie zu bewerten, stets unter Einbindung des RM-Boards.

7.3 Fazit

Die Zukunftsfähigkeit eines Unternehmens wird täglich durch zahlreiche Risiken bedroht. Neben einer konsistenten Unternehmensstrategie müssen Unternehmen daher auch eine dazu passende Risikostrategie entwickeln. Unternehmen benötigen heute jedoch nicht nur ein proaktives Risikomanagement, sondern auch ein auf die vorhandenen Risiken aufgebautes Versicherungs- und Schadenmanagement. Versicherungs- und Schadenmanagement sollten dabei integrale Bestandteile eines Risikomanagements sein.

Formal- und Sachziele des Risikomanagements werden aus den Unternehmenszielen eines Unternehmens abgeleitet und variieren dabei in ihrer Gewichtung. Während heute zunehmend Formalziele wie Ökologieverträglichkeit oder Nachhaltigkeit an Bedeutung gewinnen, bleibt ein wesentliches Sachziel im Versicherungsmanagement die Versicherbarkeit von Risiken. Eine Versicherungslösung zur Absicherung von Großrisiken kann

beispielsweise grundsätzlich als optimal im Rahmen einer Risikokostenbewertung angesehen werden. Sofern die Versicherbarkeit eines Risikos nicht in voller Höhe gewährleistet ist, muss die Lücke im Versicherungsschutz gegebenenfalls im Eigenbehalt getragen werden. Aufgabe des Risikomanagers ist es dann, im Rahmen einer Risikoanalyse das potentielle Risiko aber auch das verbleibende Restrisiko aufzuzeigen. Nicht zu unterschätzen sind auch vereinzelt auftretende Zielkonflikte zwischen Risiko- und Versicherungsmanagement, denn Unternehmen können in den einzelnen Unternehmensbereichen unterschiedliche Ziele, dargestellt in sogenannten Key-Performance-Indicators, verfolgen.

Grundsätzlich führt jedoch eine Integration des Versicherungs- in das Risikomanagement zu einer optimierten Versicherungspolitik und zu einer Minimierung der gesamten Risikokosten eines Unternehmens.

Literatur

- Anderson, B., Taylor, G., Knight, K. W., Moloney, P., Wilkinson, S., Bassett, S. et al. (2009). Risk management – Principles and guidelines. ISO 31000:2009.
- E&Y. (2019). Three Lines of Defence. Ist das Three-Lines-of-Defence-Modell eine administrative Bürde oder ein hilfreiches Modell für die Interne Revision? Hrsg. v. E&Y Wirtschaftsprüfungsgesellschaft. [https://www.ey.com/Publication/vwLUAssets/ey-interne-revision-news-three-lines-of-defence/\\$FILE/ey-interne-revision-news-three-lines-ofdefence.pdf](https://www.ey.com/Publication/vwLUAssets/ey-interne-revision-news-three-lines-of-defence/$FILE/ey-interne-revision-news-three-lines-ofdefence.pdf). Zugriffen am 02.05.2019.
- Götze, U., Henselmann, K., & Mikus, B. (2001). *Risikomanagement*. Heidelberg: Physica (Beiträge zur Unternehmensplanung). <https://doi.org/10.1007/978-3-642-57587-7>. Zugriffen am 07.08.2019.
- Haksöz, Ç. (2018). *Risk intelligent supply chains. How leading Turkish companies thrive in the age of fragility*. Boca Raton: Chapman & Hall/CRC Press.
- Hinterhuber, H. H. (Hrsg.). (1998). *Betriebliches Risikomanagement*. Wien: Verlag Österreich.
- Hopkin, P. (2012). *Fundamentals of risk management. Understanding, evaluating and implementing effective risk management* (2. Aufl.). London: Kogan Page.
- Huth, M. (2004). *Risikomanagement der Gefahrgutbeförderung. Einsatzpotential eines GIS-basierten Entscheidungsunterstützungssystems* (Gabler Edition Wissenschaft). Wiesbaden: Deutscher Universitätsverlag (Logistik und Verkehr). <https://doi.org/10.1007/978-3-322-81744-0>. Zugriffen am 13.07.2019.
- Kaiser, T., & Auer, M. (Hrsg.). (2007). *Wettbewerbsvorteil Risikomanagement. Erfolgreiche Steuerung der Strategie-, Reputations- und operationellen Risiken*. Berlin: Schmidt.
- Romeike, F., & Finke, R. B. (2003). *Erfolgsfaktor Risiko-Management. Chance für Industrie und Handel Methoden, Beispiele, Checklisten*. Wiesbaden: Gabler. <https://doi.org/10.1007/978-3-663-05715-4>. Zugriffen am 02.05.2019.
- Schmitz, T., & Wehrheim, M. (2006). *Risikomanagement. Grundlagen, Theorie, Praxis*. Stuttgart: Kohlhammer (JW).
- Strohmeier, G. (2007). *Ganzheitliches Risikomanagement in Industriebetrieben* (1. Aufl.). s.l.: DUV Deutscher Universitätsverlag (Techno-ökonomische Forschung und Praxis). <http://gbv.eblib.com/patron/FullRecord.aspx?p=751808>. Zugriffen am 13.05.2019.
- The Institute of Risk Management. (2011). Risk appetite and tolerance. Executive Summary. Hrsg. v. The Institute of Risk Management. https://www.theirm.org/media/3779216/64355_Riskapp_A4_web.pdf. Zugriffen am 18.07.2019.

- Welge, M. K., & Eulerich, M. (2014). *Corporate-Governance-Management. Theorie und Praxis der guten Unternehmensführung* (2. Aufl). Wiesbaden: Springer Gabler. <https://doi.org/10.1007/978-3-8349-4539-6>. Zugegriffen am 03.09.2019.
- Wolf, K., & Runzheimer, B. (2003). *Risikomanagement und KonTraG. Konzeption und Implementierung* (4., vollst. überarb. u. erw. Aufl.). Wiesbaden: Gabler.

Detlef Hesse; Geb. 1958, Dipl. Ingenieur, Studium Maschinenbau, Fachrichtung Verfahrenstechnik an der RWTH Aachen. Seit 1999 Risikomanager bei AB Electrolux in verschiedenen Positionen, unter anderem als Global Property Risk & Insurance Manager und als Sektor/Regional Risk Manager Europe. Davor war Herr Hesse als Leiter des Bereichs Risikovorsorge eines Unternehmens der Versicherungswirtschaft sowie als Projekt ingenieur in der Industrie tätig, unter anderem zuständig für die Erstellung von Risikoanalysen sowie Sicherheitsanalysen nach StörfallVO.

Fabio Papa; Von 2009–2015 Studium an der Universität Siegen (Mathematik und analytische Philosophie). Von 2016–2019 Studium an der TH Köln im Fach Versicherungswesen (B.Sc.). Seit 2016 bei der RheinLand Versicherungsgruppe in Neuss. Von September 2019 bis Dezember 2019 Vorstandsstab. Seit Januar 2020 in der Einheit Strategie Versicherungsgeschäft. Tätigkeitsfelder sind Business Controlling und Strategie.



Technisches Risikomanagement

8

Die besondere Relevanz von Lieferantenaudits in Bezug auf Lieferantenausfälle und Betriebsunterbrechungen

Thomas Bär und Yannick Berkemeier

Zusammenfassung

Im Vergleich zum finanziellen Risikomanagement wird das technische Risikomanagement in vielen Unternehmen weniger beachtet. Dabei stellt dieses einen essenziellen Part des Risikomanagements dar. Insbesondere größere Unternehmen, die hohe Abhängigkeiten gegenüber Lieferanten aufweisen, führen Lieferantenaudits durch, in denen die technischen Risiken der Lieferanten identifiziert, analysiert, bewertet und schließlich mittels geeigneter Maßnahmen behandelt werden. Hierdurch sinkt das für Unternehmen mitunter existenzielle Risiko von Lieferantenausfällen. Der Ausfall eines single source bzw. single quality suppliers kann dazu führen, dass die eigene Wertschöpfungskette und damit die gesamte Leistungserstellung unterbrochen wird.

8.1 Einleitung

Die enormen Veränderungsgeschwindigkeiten bedingen, dass strategische und betriebswirtschaftliche Entscheidungen der Unternehmensführer in immer kürzeren Zeiträumen auf Grundlage weniger Informationen getroffen werden. Zusätzlich müssen die Entscheidungen konsistent mit den Compliance Richtlinien sowie den ethischen Ansprüchen sein und den behördlichen Anforderungen genügen. Darüber hinaus sind die nationalen und

T. Bär (✉)

Bär Consulting, Riesweiler, Deutschland

E-Mail: t.baer@risk-consult.biz

Y. Berkemeier

TH Köln, Institut für Versicherungswesen, Köln, Deutschland

E-Mail: yannick.berkemeier@isokoeln.de

internationalen Gesetze und Vorschriften einzuhalten. In diesem Handlungsrahmen ist es eine große Herausforderung für die Unternehmen, auf dem globalen Markt hochwertige Produkte termingerecht zu wettbewerbsfähigen Preisen zu produzieren und an den Kunden zu liefern.

Die hohe Veränderungsgeschwindigkeit der Marktumfelder bedingt darüber hinaus, dass auch die Vernetzung der Kunden- und Lieferantenbeziehungen immer komplexer werden, beispielsweise durch die Anbindung von Systemen per EDI-Schnittstelle oder über Portale. Gleichzeitig erfordert die nachhaltige Sicherung der Wettbewerbsfähigkeit eines Unternehmens, dass die unternehmenseigenen Kernkompetenzen weiter ausgebaut werden und die Unternehmen sich strategisch nach diesen ausrichten. Aufgrund dessen steigt die Abhängigkeit von Zulieferern, unabhängig davon, ob diese Rohstoffe, Halb fertigprodukte oder Dienstleistungen zur Verfügung stellen.

Da sich nahezu alle Industrieunternehmen oder Gewerbebetriebe in dem gleichen sich dynamisch verändernden wirtschaftlichen Umfeld befinden und einem hohen Wettbewerbsdruck ausgesetzt sind, sind interne oder externe Fehler, die signifikanten Einfluss auf die Wertschöpfungskette in einem Unternehmen haben, nicht zu akzeptieren und im Falle des Eintritts nur sehr schwer zu kompensieren.

In diesem komplexen Marktumfeld können Industrie- und Gewerbeunternehmen nur nachhaltig erfolgreich sein, wenn sie über gute Informationen verfügen. Belastbare Informationen sind die Basis für gute Entscheidungen. Auch primär als negativ angesehene Nachrichten können gute Informationen in dem Prozess sein. Verlässliche, objektive und verwertbare Informationen stellen für ein Unternehmen einen Wettbewerbsvorteil dar. Eine gute Qualität der Informationen bildet die Grundlage für ein erfolgreiches unternehmerisches Risikomanagement.

Der Einkauf gehört zu den wichtigsten Generatoren für den Unternehmenserfolg. Im Rahmen dessen sind alle notwendigen Güter, welche zur Wertschöpfung notwendig sind, zur richtigen Zeit, mit der richtigen Qualität und zum bestmöglichen Preis zu besorgen. Die Verfügbarkeit von Lieferanten hinsichtlich der folgenden beispielhaften Aspekte ist die Basis des Unternehmenserfolgs:

- Produktqualität
- Preis
- Timing
- Compliance
- Ethik
- Loyalität
- Image

Die Konzentration auf das Kerngeschäft, die Spezialisierung und die Globalisierung bewirken, dass die Anzahl der sogenannte *Single source* und *single quality supplier*, (alleinige Lieferanten von Produkten und Lieferanten, die ein speziell gefordertes Produkt oder eine bestimmte Qualität liefern) steigt. Industrie- und Gewerbeunternehmen beziehen

heute durchschnittlich 30 Prozent ihrer Rohstoffe oder Halbfertigprodukte von single source oder single quality Lieferanten. Darüber hinaus werden derartige Abhängigkeiten im Rahmen der Industrie 4.0 weiter ansteigen. Zulieferer wachsen aufgrund der steigenden digitalen Vernetzung noch enger mit den Unternehmen zusammen und werden vollständig in deren Wertschöpfungskette integriert. Dies führt dazu, dass der Austausch von Lieferanten weiter erschwert wird (vgl. Schlatt 2016). Ein Lieferantenausfall stellt daher eine Gefahr für Unternehmen dar, weil dieser den Produktionsprozess stört und gegebenenfalls eine Betriebsunterbrechung mit erheblichen finanziellen Verlusten und Einnbußen bei der Kundenzufriedenheit bewirkt.

Insofern verwundert es nicht, dass insbesondere große Unternehmen im Rahmen des technischen Risikomanagements die wichtigsten Lieferanten überprüfen, um Lieferantenausfällen präventiv entgegenzuwirken. Aufgrund dessen thematisiert diese Arbeit das technische Risikomanagement in Verbindung mit Lieferantenaudits unter spezieller Berücksichtigung des Betriebsunterbrechungsrisikos.

8.2 Begriffsbestimmung

8.2.1 Definition des „Technischen Risikomanagements“

Unter dem Begriff des allgemeinen Risikomanagements wird der systematische und zielgerichtete Umgang mit aktuellen und potenziellen Risiken eines Unternehmens beschrieben. Der Risikomanagementprozess umfasst die Identifikation, Analyse und Bewertung von Risiken sowie die daraus abgeleiteten Maßnahmen zur Beseitigung oder Minimierung dieser. Weiter erfolgt im Rahmen des Risikomanagements die laufende Überwachung der Risiken (vgl. Rohlfs 2018, S. 1). Die Grundlage der Zielsetzung des Risikomanagements bilden die übergeordneten Unternehmensziele. In der Regel können diese in leistungswirtschaftliche, finanzielle, soziale und ökologische Ziele unterteilt werden. Zur Erreichung dieser Ziele ist das Management verantwortlich, welches auf operativer Ebene eine Vielzahl von Entscheidungen trifft, um den Unternehmenserfolg und die langfristige Unternehmenswertsteigerung sicherzustellen. Mit Entscheidungen gehen jedoch regelmäßig Unsicherheiten und Risiken einher, welche die Unternehmensziele gefährden können. Entsprechend ist das Risikomanagement unmittelbar der Unternehmensführung zuzuordnen, da diese im Rahmen der Unternehmenssteuerung Risiken systematisch bearbeiten und kontrollieren muss (vgl. Diedrichs 2018, S. 10).

Das Risikomanagement gehört häufig den Bereichen *Controlling* oder *Financial and Treasury* innerhalb der Unternehmen an. Das technische Risikomanagement stellt hingegen einen ergänzenden Part zum Risikomanagement dar. Im Rahmen des technischen Risikomanagements stehen folgende Felder im Fokus (vgl. Hagebölling 2009a, S. 32):

- Produktionsstandort
- Anlagentechnik & Produktionsmaschinen

- Lagerbereiche
- Technische Infrastruktur
- Ausfallszenarien, Reparatur- und Ausfallzeiten
- Organisatorische Abläufe

Das technische Risikomanagement, welches auch als Risk Engineering bezeichnet wird, umfasst alle technischen Zusammenhänge und technischen Parameter. Hierbei werden nicht lediglich die technischen Anlagen, sondern darüber hinaus das Gesamtumfeld des Unternehmens betrachtet. Dieses umfasst alle Betriebsstätten und Standorte inklusive der einzelnen Wechsel- und Rückwirkungen (vgl. Hagebölling 2009a, S. 32).

Das Ziel des technischen Risikomanagements ist der systematische Umgang mit potenziellen und bereits vorliegenden Risiken, welche den Produkterfolg, beginnend bei der Entwicklung bis hin zur Herstellung, gefährden. Risiken, die das Produkt sowie dessen gesamten Herstellungsprozess betreffen, sollen somit frühzeitig erkannt und mittels geeigneter Maßnahmen beseitigt, gemindert oder kontrolliert werden (vgl. Zentis et al. 2012, S. 256).

8.2.2 Technisches Risiko

Die Technik setzt sich zusammen aus den genutzten Geräten, Maschinen sowie Anlagen und wird in Kombination mit dem dafür notwendigen menschlichen Handeln als technisches System bezeichnet (vgl. Wagner 2000, S. 130).

Eine einheitliche Definition für das technische Risiko gibt es nicht. Der Begriff des technischen Risikos wird häufig im Zusammenhang mit dem Qualitätsmanagement und dem reinen Produkt eines Unternehmens verstanden und definiert. So beschreiben technische Risiken die möglichen Fehler, welche die Produktion und die Qualität des Produktes gefährden (vgl. Zentis et al. 2011, S. 11). Diese Unsicherheiten bestehen nicht nur bei der Entwicklung und Produktion, sondern auch im Rahmen der Nutzung des erstellten Produkts. Begründet werden technische Risiken unter anderem durch die Komplexität der Produkte und neuartig anzuwendende Techniken (vgl. Schnorrenberg und Goebels 1997, S. 11).

Für den Zweck des ganzheitlichen technischen Risikomanagements eignet sich die Definition von Zentis et al., da diese einerseits den Zusammenhang zwischen Qualitäts- und Risikomanagement abbildet. Allerdings ist diesbezüglich anzumerken, dass der Begriff des Fehlers nicht weiter definiert wird, sodass die Definition ein breites Spektrum von Ursachen bzw. Quellen technischer Risiken zulässt. So sind neben den unmittelbaren Ursachen, wie die Fehlbedienung einer Maschine durch den Mitarbeitenden, auch die mittelbaren Ursachen, wie zum Beispiel Umwelteinwirkungen in Verbindung mit unzureichenden Sicherungsmaßnahmen, erfasst.

8.3 Relevanz des technischen Risikomanagements für Unternehmen

Technische Risiken sind besonders für produzierende Unternehmen von hoher Relevanz und können den Unternehmenserfolg maßgeblich negativ beeinflussen. In der Praxis zeigt sich jedoch, dass die Beachtung technischer Risiken und die Einführung eines ganzheitlichen technischen Risikomanagements als Ergänzung zum allgemeinen Risikomanagement eine untergeordnete Rolle spielen. Häufig begründet sich dies in mangelndem technischem Know-how sowie fehlenden zeitlichen und finanziellen Ressourcen.

Beispielhaft sind das japanische Seebeben und die Zerstörung des Atomkraftwerks in **Fukushima** in 2010 zu nennen. Infolge des Seebebens entstanden bis zu 15 Meter hohe Tsunamiwellen. Die zur Meerseite gelegenen Schutzmauern wurden überspült und das gesamte Gelände des Kraftwerks überflutet. Hierdurch kam es zum Ausfall der Notstromaggregate sowie Wasserpumpen, welche die notwendige Kühlung der Reaktoren sicherstellten. Durch den Ausfall des Kühlsystems kam es schließlich zur Kernschmelze sowie mehreren Explosionen. Der Tsunamischutz wurde ursprünglich auf Basis einer in den Sechzigerjahren sich ereigneten Tsunamiwelle in Chile auf 3,1 Meter angelegt. Später wurde die Schutzmauer auf 5,7 Meter aufgestockt. Hingegen hat die International Atomic Energy Agency als Empfehlung das 10.000-jährige Höchstereignis als Bezugspunkt ausgesprochen. Dokumentiert sind seit 1498 weltweit jedoch mindestens zwölf Tsunamis mit einer Amplitude von mehr als zehn Metern und sechs Tsunamis mit einer Amplitude von mehr als 20 Metern (vgl. Preiss 2017, S. 50 ff.).

Ebenfalls durch erhebliche technische Mängel verursacht, waren die Explosion und der Brand der Ölbohrplattform **Deepwater Horizon** im mexikanischen Golf in 2010. Es kam zum *Blowout*, einem plötzlichen Austritt von Gasen und Ölen, welcher im Normalfall durch eine Schutzvorrichtung, dem Blowout-Preventer, vermieden wird. Die Gase entzündeten sich und es kam zur Explosion. Im Nachgang zu dem Unglück wurde festgestellt, dass der Blowout-Preventer erhebliche Mängel aufwies, welche der Grund für das Versagen der Vorrichtung gewesen sind (vgl. Preiss 2017, S. 39 ff.). In der Folge traten über Monate mehrere Millionen Barrel Öl aus, die zu erheblichen Umweltschäden führten. In den USA wurde der Energiekonzern BP deshalb verurteilt und musste erhebliche Strafzahlungen tätigen. Insgesamt hat der Unfall das Unternehmen ca. 62 Milliarden US-Dollar gekostet (vgl. Kaiser 2016).

Nicht nur der Sachschaden infolge einer sich realisierenden Gefährdung, sondern insbesondere Betriebsunterbrechungen stellen für Unternehmen ein erhebliches Risiko dar. Abhängig von den individuellen Gegebenheiten im Schadenfall sowie von der Unternehmensart kann das Verhältnis zwischen dem Anteil des Sachschadens und des Betriebsunterbrechungsschadens am Gesamtschaden stark abweichen. So ist der Betriebsunterbrechungsschaden bei Chemiebetrieben in der Regel wesentlich größer als der eigentliche Sachschaden.

Zwar lassen sich die finanziellen Risiken eines Sachschadens sowie der daraus resultierenden Betriebsunterbrechung auf Versicherungsunternehmen transferieren, das Erreichen

der ursprünglichen Wirtschaftskraft wie vor dem Schaden gelingt jedoch nur 23 Prozent der Unternehmen. 43 Prozent der betroffenen Unternehmen führen den Betrieb in der ursprünglichen Form nicht mehr fort, sechs Prozent der Unternehmen werden verkauft und 28 Prozent der Unternehmen haben innerhalb von drei Jahren Insolvenz anmelden müssen (vgl. Jörgl 2009, S. 55).

8.4 Rechtliche Grundlagen

Auch der Gesetzgeber manifestiert auf nationaler Ebene die Relevanz des Risikomanagements mittels diverser Gesetze. Beispielsweise kann hier das am 01.05.1998 in Kraft getretene Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) genannt werden. Infolge namhafter Unternehmensinsolvenzen beabsichtigt das Gesetz, dass Unternehmen Risikomanagementsysteme implementieren, um bestandsgefährdende Risiken frühzeitig zu erkennen und abzuwehren. Dies trägt einerseits zur Verbesserung der Bewertbarkeit von Unternehmensprojekten und -zielen bei, andererseits steigt die Transparenz gegenüber Gläubigern, Anlegern und Investoren in Bezug auf wertbeeinflussende Risiken. Zusammenfassend wird durch das KonTraG die bessere Überprüfung der eigenen Investitionsentscheidungen ermöglicht (vgl. Hommelhoff und Mattheus 2000, S. 8).

Der sorgfältige Umgang basiert dabei auf zwei Säulen. Nach § 91 Abs. 2 AktG hat der Vorstand Maßnahmen zu treffen, die dazu geeignet sind gefährdende Entwicklungen frühzeitig zu erkennen. Darüber hinaus sind nach § 289 Abs. 1 HGB im Rahmen des Lageberichts die Entwicklung sowie die wesentlichen Risiken für die Zukunft des Unternehmens zu beurteilen und zu erläutern. Sowohl das Risikomanagementsystem als auch die Angaben im Lagebericht werden durch den Wirtschaftsprüfer kontrolliert. Das Ziel des Gesetzgebers ist es, die Unternehmensprozesse transparenter und die Handlungen sowie die Berichterstattung des Unternehmens glaubwürdiger zu machen (vgl. Glage und Grötzner 2016, Rn. 17).

Auf internationaler Ebene wurden die Grundsätze und Richtlinien für das Risikomanagement erstmalig in der Norm ISO 31000 beschrieben. Diese beinhaltet generische Informationen und drückt die Anforderungen als Empfehlungen aus (vgl. Zentis 2013, S. 36). Gemäß den Einleitungsworten der ISO 31000 (2011-01-00) wird nicht auf die Anforderung von speziellen Wirtschaftszweigen oder spezifische Risiken abgezielt. Der Fokus liegt vielmehr auf der Einführung konsistenter Prozesse, die eine wirksame, effiziente und kohärente Behandlung von Risiken organisationsweit sicherstellen. Im Kontext dieser Arbeit bezieht sich die Norm somit nicht explizit auf technische Risiken, sondern das allgemeine Risikomanagement.

Inhaltlich nimmt die Norm wesentliche Inhalte der bereits in 2004 erschienenen ersten Ausgabe des österreichischen Standards ONR-Serie 49.000 „Risikomanagement für Organisationen und Systeme“. Die dritte Version der österreichischen Norm hat die Inhalte der ISO 31000 schließlich vollständig inkludiert (vgl. Brühwiler und Romeike 2010,

S. 87 f.). Die österreichische ONR-Serie 49.000 stellt mehrere aufeinander aufbauende Normen dar, welche im Vergleich zur ISO 31000 als Anforderungen formuliert werden und somit Zertifizierungen nach dieser Norm ermöglichen (vgl. Zentis 2013, S. 36). Abb. 8.1 stellt die Struktur der ONR-Serie 49.000 ff. dar.

Über die allgemeinen Risikomanagement-Normen hinaus gibt es weitere branchenspezifische Normen, wie die DIN EN ISO 14971 „Anwendung des Risikomanagements auf Medizinprodukte“ oder die ISO TS 16949 „Besondere Anforderungen bei Anwendung der ISO 9001 für Serien- und Ersatzteilproduktion in der Automobilindustrie“, welche jedoch nicht weiter thematisiert werden.



Abb. 8.1 Struktur der ONR-Serie 49.000 ff. (Quelle: eigene Darstellung in Anlehnung an Austrian Standards 2014, S. 3)

8.5 Technischer Risikomanagementprozess

Auch für das technische Risikomanagement bildet der Risikomanagementprozess gemäß der DIN ISO 31.000 die Grundlage. Im Sinne der Norm ist der Risikomanagementprozess im Rahmen des Managements und der Entscheidungsfindung in die Strukturen, Abläufe sowie Prozesse des Unternehmens vollständig integriert. Abb. 8.2 nimmt diese Kernprozesse auf und bildet die Struktur der DIN ISO 31000 ab.

Ein wirksames technisches Risikomanagement ist ebenso wie das finanzielle Risikomanagement ein integraler Bestandteil der Prozesse und Entscheidungsfindungen. Hierzu zählt, dass im Rahmen der Kommunikation sichergestellt ist, dass die wesentlichen Stakeholder ein Risikobewusstsein aufbauen und Risiken bei der Entscheidungsfindung berücksichtigen. Um die Qualität und Wirksamkeit des technischen Risikomanagements zu wahren und laufend zu überprüfen, sind entsprechende Kontrollmechanismen zu integrieren. Das

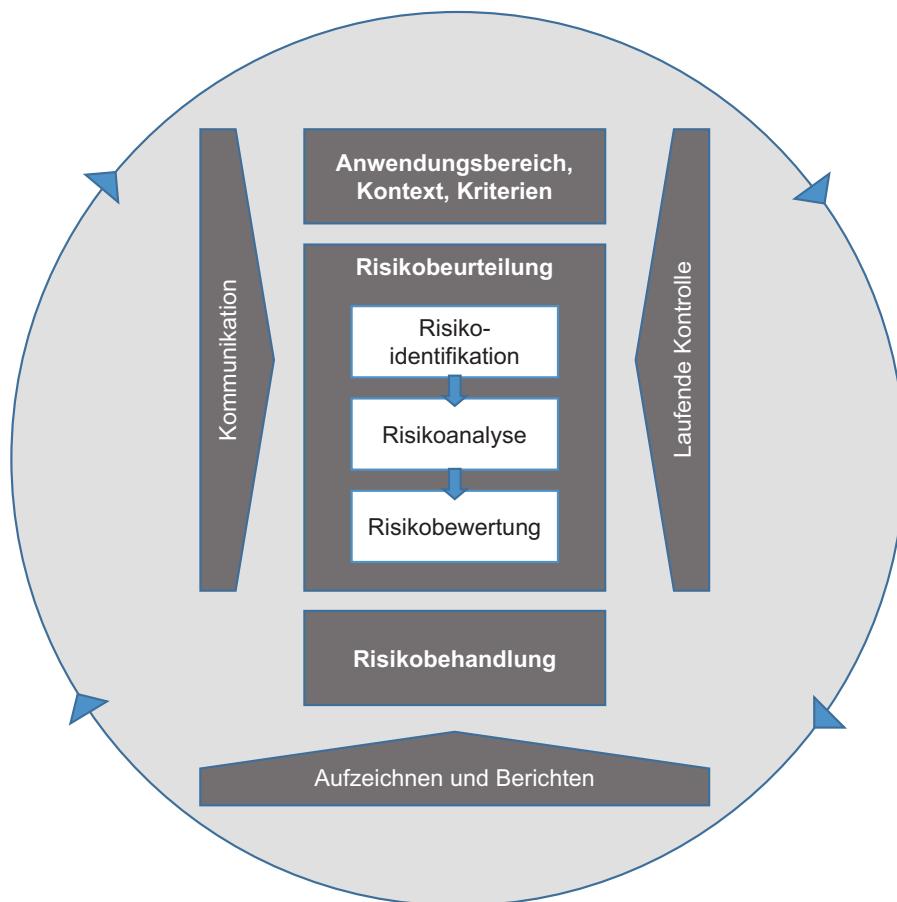


Abb. 8.2 Risikomanagementprozess nach DIN ISO 31000. (Quelle: eigene Darstellung in Anlehnung an DIN 2018, S. 16)

Aufzeichnen und Berichten des Prozesses sowie dessen Ergebnisse wirken unterstützend bei der Kommunikation und Kontrolle sowie bei der Interaktion mit Stakeholdern inklusive derer, denen gegenüber die verantwortlichen Personen rechenschaftspflichtig sind (vgl. DIN 2015, S. 59). Als Abgrenzung zum finanziellen Risikomanagement, werden für das technische Risikomanagement der rein technische Teil und damit einhergehend alle Risiken des Produktionsprozesses als Anwendungsbereich vorgegeben. Diese Abgrenzung bildet den Anwendungsbereich bzw. Kontext des technischen Risikomanagements (vgl. Hagebölling 2009b, S. 20).

8.5.1 Risikoidentifizierung und -analyse

Zur Identifizierung und Analyse der technischen Risikosituation eines Unternehmens bedarf es qualifizierter Prüfer, die über ein hohes technisches Know-How verfügen. Darüber hinaus bestehen im Rahmen der Prüfungen hohe Anforderungen an die Unabhängigkeit und Sachlichkeit der Ergebnisse. Für diesen Zweck eignet sich insbesondere die Durchführung von Audits.

Bei den Audits im Rahmen des technischen Risikomanagements kann zwischen internen und externen Audits unterschieden werden. Interne Audits bzw. first-party-audits werden innerhalb einer Organisation durchgeführt und erfüllen unternehmensinterne Absichten. Sie werden üblicherweise durch das Management in Auftrag gegeben. Hierbei sind die Ansprüche an ein Audit in Bezug auf Sachlichkeit und Unabhängigkeit zu wahren. Die Durchführung des Audits kann sowohl durch interne als auch externe Prüfer erfolgen. Besonders bei Auditierungen, deren Inhalte die vorhandenen Kompetenzen innerhalb des Unternehmens überschreiten oder bei denen eine entsprechende Unabhängigkeit durch interne Mitarbeitende nicht gewährleistet werden kann, ist der Einsatz externer Berater notwendig.

Second-party-audits gehören zu den externen Audits und werden üblicherweise durch Kunden eines Lieferanten in Auftrag gegeben. Sie werden deshalb auch als Lieferantenaudits bezeichnet. Die Prüfung erfolgt durch externe Auditoren. Das Ziel des Kunden im Rahmen der technischen Audits ist es, die technischen Gegebenheiten und Gefahren der Lieferanten zu identifizieren und entsprechende Auflagen bzw. Gegenmaßnahmen einzuleiten. Dies erfolgt vor dem Hintergrund, dass die eigene Leistungserstellung der Kunden unmittelbar von der pünktlichen und sachgerechten Lieferung abhängt. Lieferausfälle infolge technischer Defekte an Maschinen oder Brände können erhebliche wirtschaftliche Auswirkungen haben. Die Art der Lieferantenaudits ist vielschichtig und hängt von den Interessen der Kunden ab. Neben der technischen Überprüfung können auch Anforderungen an die Produktqualität, Arbeitssicherheit etc. im Vordergrund stehen. Branchenübergreifende Regelungen, die zwingend anzuwenden sind, gibt es für Lieferantenaudits nicht, jedoch können spezifische Normen, wie zum Beispiel die VDA 6.1, welcher die Qualitätsstandards für Automobilzulieferer festlegt, angewendet werden.

Darüber hinaus gibt es sogenannte Third Party Audits. Hierbei handelt es sich um Zertifizierungsprüfungen, welche nicht durch interne Mitarbeitende, sondern immer durch externe Dritte erfolgen (vgl. Abb. 8.3; vgl. Gietl und Lobinger 2016, S. 10 ff.).

Die Inhalte des technischen Audits hängen stark von den Zielen des Auftraggebers ab. Die in Tab. 8.1 dargestellten Inhalte bzw. Risikoparameter können beispielsweise Bestandteil eines technischen Lieferantenaudits sein. Diese werden mittels einzelner Beispiele beschrieben:

Im Anschluss an die ganzheitliche Identifikation der technischen Risiken, bedarf es der Bewertung dieser, um die einzelnen Gefährdungen vergleichbar zu machen und diese in ihrer Priorität zu kategorisieren.

8.5.2 Risikobeurteilung

Für alle genannten Gefährdungsparameter sind Szenarien durchzuspielen und die Auswirkungen auf das Unternehmen in Bezug auf mögliche Sach- und/oder Betriebsunterbrechungsschäden zu ermitteln.

Grundsätzlich lässt sich das Risiko als Produkt aus der quantitativen Schadenhöhe und Eintrittswahrscheinlichkeit des Ereignisses definieren. In Bezug auf die Bewertung des Betriebsunterbrechungsrisikos infolge des Lieferantenausfalls bedarf es demnach der Ermittlung der Ausfallwahrscheinlichkeiten infolge unterschiedlicher Szenarien sowie der damit verbundenen Schadenhöhen. Die Schadenhöhe kombiniert dabei die Ausfallzeiten

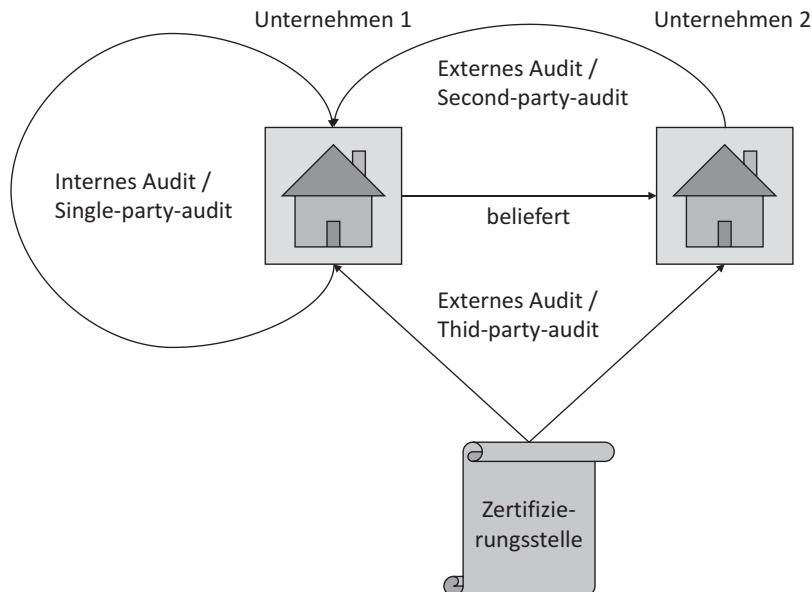


Abb. 8.3 Durchführung von Audits. (Quelle: eigene Darstellung)

Tab. 8.1 Mögliche Prüfungsinhalte eines technischen Audits

Allgemeine Informationen	<ul style="list-style-type: none"> - Gründung, Betriebsstandorte, Hauptprodukte - Zahl der Mitarbeitenden - Eigentümerstruktur - Umsätze
Betriebsstandort	<ul style="list-style-type: none"> - Regionale Einordnung → ggf. politische Instabilitäten oder geringe gesetzliche Anforderungen an die betriebliche Sicherheit - Allgemeine Infrastruktur (Straßen, Schifffahrtswege, Bahn etc.) → mögliche Abhängigkeiten von einzelnen Transportwegen - Grundstücksfläche, Gebäudeflächen, Lagerflächen im Freien - Zustand und Wartung der Gebäude - Nachbarschaftsgrundstücke → ggf. feuergefährliche Betriebe
Produktion	<ul style="list-style-type: none"> - Allgemeine Beschreibung - Verwendete Rohstoffe & Halbfertigprodukte, Abnahmemengen und Zulieferer sowie Lieferzeiten - Risikoreiche/Feuergefährliche Arbeiten (z. B. Schweißen) - Zustand der Produktionsanlagen → Identifizierung von Maschinen, deren Ausfall zu einer Produktionsunterbrechung führt (sog. <i>Bottlenecks</i>) - Zustand der Hilfsmaschinen (z. B. Radlader) - Überprüfung auf Redundanzen bzgl. kritischer Produktionsanlagen sowie Hilfsmaschinen, Ersatzteillagerung für Reparaturen, Serviceverträge mit Herstellern, sodass langfristige Einschränkung der Produktion vermieden wird - Mögliche interne Ausweichstandorte im Falle einer Betriebsunterbrechung oder externe Alternativen durch vertragliche Vereinbarungen mit anderen Unternehmen - Gelagerte Vorräte (ggf. feuergefährliche Stoffe, Verpackungsmaterialien), Art der Vorratslagerung (freie Lagerflächen, Hochregallager etc.)
Personal	<ul style="list-style-type: none"> - Menschliche Fehler sind häufig Ursächlich für Schäden → Motivation und Qualifikation sind daher wichtige Indikatoren zur Beurteilung dieser → Qualifikationen, Weiterbildungsmöglichkeiten & Fluktuation
Qualitätsmanagement	<ul style="list-style-type: none"> - Überprüfung, ob Zertifizierungen zum Qualitätsmanagement vorliegen - Überprüfung, ob die Qualität der eingehenden Rohstoffe und Halbfertigprodukte, welche in die herzustellenden Produkte einfließen, kontrolliert wird - Durchführungen von Kontrollen und Dokumentierungen der einzelnen Produktionsschritte - Lösungsorientierte Fehlerkultur

(Fortsetzung)

Tab. 8.1 (Fortsetzung)

Ver- und Entsorgung	<ul style="list-style-type: none"> - Betriebsmittel (z. B. Strom, Druckluft, Wasser, Gase, Heiß- und Kaltluft) - Überprüfung denkbarer Szenarien zu Versorgungsausfällen (Elektrizitätsnetz ohne Redundanzen, marode Kabeltunnel, einzelne Transformatoren oder Wasserpumpen etc.) - Ggf. Umgang mit speziellen Abfallprodukten oder Brauchwasser
Naturgefahren	<ul style="list-style-type: none"> - Sturm-, Flut- oder Erbebengebiete - Beurteilung der Vulnerabilität gegenüber Starkregenereignissen mit Oberflächenwasser von 10 bis 20 cm auf dem Betriebsgelände - Auswirkung von Dürreereignissen auf den Betrieb
Feuer	<ul style="list-style-type: none"> - Feuer- und explosionsgefährliche Produktionsschritte/ Industriezweige (Recycling, Bäckerei, Mastbetriebe, Holzverarbeitung etc.) - Bausubstanz - Lagerung/Verarbeitung feuergefährlicher Stoffe - Zustand der elektrischen Anlagen - Zustand der Kabeltunnel - Bestehende Branderkennungs- und -bekämpfungsanlagen
Lieferanten- und Kundenausfall	<ul style="list-style-type: none"> - Analyse der größten Vulnerabilitäten in der Wertschöpfungskette (Großkunden, single source oder single quality Lieferanten) - Beurteilung von Wechselwirkungen zwischen einzelnen Betrieben innerhalb eines Unternehmens, d. h. die Folgen einer Betriebsunterbrechung auf weitere Betriebe des Unternehmens
Einbruchschutz	<ul style="list-style-type: none"> - Zutrittsschutz vor Unbefugten Dritten - Identifizierung und Überprüfung der technischen Schutzaufbauten
Cyber	<ul style="list-style-type: none"> - Nutzerauthentifizierungen/Passwortschutz/Zugangsberechtigungen etc. - Schutzsysteme (Firewalls, Antivirenprogramme) - Server-Backups - Aufklärung der Mitarbeitenden in Bezug auf Cybergefahren

für die einzelnen Szenarien sowie die damit einhergehenden Ertragsverluste. Darüber hinaus sind jedoch weitere mittelbare Folgen, wie Reputations-, Kunden- sowie Marktanteilsverluste, Vertragsstrafen und Abgänge von Kapitalgebern zu beachten.

Regelmäßig verfügen Unternehmen nicht oder nur unzureichend über Informationen zu den eigenen Ausfallwahrscheinlichkeiten der Produktionsanlagen, Versorgungseinrichtungen oder der IT sowie den daraus resultierenden Auswirkungen für den Betrieb. Insofern ist die Informationslage in Bezug auf die technischen Gegebenheiten bei Zulieferern umso ungewisser. Obwohl die Wahrscheinlichkeit des Eintritts von Betriebsstörungen und entstehenden Betriebsunterbrechungen gering ist, müssen diese im Rahmen des technischen Risikomanagements erfasst werden. Denn erst auf Basis der Informationen zu den Auswirkungen einzelner Szenarien lassen sich sinnvolle Bewertungen durchführen und Gefahren mit einem relevanten Betriebsunterbrechungsrisiko für den Betrieb vergleichbar machen. Zur Bewertung der einzelnen Auswirkungen der verschiedenen Unterbrechungs-

szenarien sind Teams mit unterschiedlichen Mitarbeitenden notwendig. Dabei sind abhängig von der Größe des Unternehmens die Mitarbeitenden aus verschiedenen Bereichen, wie Einkauf, Verkauf, Controlling, Sicherheit und Qualitätssicherung, Ent- und Versorgung, Recht und Betrieb sowie Vertreter des Managements zu involvieren (vgl. Hagebölling 2009a, S. 39 ff.). Im Rahmen des technischen Audits können die notwendigen Informationen mittels Befragungen während der Standortbesichtigung, Checklisten und Fragebögen erhoben werden.

8.5.3 Risikobehandlung

Im Anschluss an die Risikobeurteilung erfolgt die Risikobehandlung. Beim Lieferantenaudit erhält der Auftraggeber das Gutachten des Auditors. Darin enthalten sind eine detaillierte Beschreibung der technischen Risikosituation sowie Empfehlungen zur Bearbeitung der technischen Risiken. Auf Basis des Gutachtens fordert der Auftraggeber seinen Lieferanten auf, die wesentlichen Mängel zu beseitigen. Hierbei ist zwischen technischen und organisatorischen Maßnahmen zur Optimierung der Risikosituation zu unterscheiden.

8.5.3.1 Technische Maßnahmen

Der Einsatz technischer Maßnahmen eignet sich vorwiegend für die Gefährdungsparameter *Naturgefahren*, *Feuer*, *Versorgung*, *Cyber* und *Einbruch- bzw. Zutrittsschutz*. Beispielaft werden nachstehend technische Maßnahmen zu den einzelnen Gefahren genannt und erklärt.

Naturgefahren

Liegt der Betrieb innerhalb eines für Überschwemmungen anfälligen Gebietes ohne erhöhte Lage, sodass Überschwemmungen durch Hochwasser oder Starkregen den Betrieb unmittelbar betreffen, sind im Rahmen des technischen Risikomanagements Maßnahmen einzuleiten, die das Risiko eines Sachschadens sowie einer daraus resultierenden Betriebsunterbrechung reduzieren.

Grundsätzlich sollte hinsichtlich Überschwemmungen bei der Auswahl der Maßnahmen das 500-Jahres-Ereignis als Vergleichswert herangezogen werden. Mittels Wahrscheinlichkeitsverteilungen wird also beurteilt, welches Überschwemmungereignis lediglich mit einer Wahrscheinlichkeit von 0,2 Prozent pro Jahr eintritt (vgl. FM Global 2016, S. 4). Auf Basis dessen ist zu überprüfen, welche Wasserstände infolge von Starkregenereignissen und/oder Überschwemmungen auf dem Betriebsgelände möglich sind.

Für den Schutz der Gebäude ist darauf zu achten, dass flut-/wasserresistente Baustoffe sowie schnell zu reinigende Materialien verwendet werden. In stark gefährdeten Regionen ist zu prüfen, ob bauliche Schutzmaßnahmen wie das Errichten eines Dammes, einer Flutmauer mit entsprechender Torvorrichtung oder Hochwasserklappen für Türen sinnvoll sind. Darüber hinaus sind der Zustand und die Kapazitäten der Entwässerungssysteme in Bezug auf den Bedarf beim Eintritt des 500-Jahres-Ereignisses zu kontrollieren. Es sollten

jedoch mindestens Produktionslinien, Maschinen, Lager bzw. Vorräte und Transformatoren etc., welche essenziell für die Betriebsfähigkeit sind, durch bauliche Maßnahmen angehoben oder in höhere Etagen verlegt werden, sodass eine Überflutung des Betriebs toleriert werden kann (vgl. FM Global 2016, S. 4 ff.).

Im Rahmen des Schutzes vor Sturmereignissen ist die regelmäßige Wartung und Instandhaltung des Betriebsgebäudes elementar. Insbesondere Dächer, Fassaden und Außenwände verlieren ihre Widerstandsfähigkeit, wenn diese Mängel oder Schäden aufweisen. Öffnungen führen darüber hinaus zu mehr Angriffsfläche für den Sturm und entsprechend zu größeren Schäden.

Bei Solar- und Photovoltaikanlagen ist eine ausreichende Sicherung und Verankerung zu wahren. Hierbei ist zu beachten, dass sich die Herstellerangaben zur Windbelastbarkeit häufig auf Mittelwerte beziehen. Spitzenböen hingegen können fast das Doppelte dieser Mittelwerte erreichen. Bäume, welche sich auf dem und um das Betriebsgelände befinden, sollten regelmäßig überprüft werden, da diese im Falle eines Umsturzes Beschädigungen an Gebäuden oder empfindlichen Infrastrukturen hervorrufen können (vgl. GDV 2016, S. 16). In Gebieten, die von Hurricanes oder Taifunen betroffen sind, sind kurz vor einem Sturm zusätzliche Maßnahmen, wie das Verbarrikadieren von Fenstern, zu empfehlen.

Feuer

Grundsätzlich sind im Sinne des Brandschutzes bei der Errichtung von Betrieben Baustoffe zu verwenden, die bezüglich der Brennbarkeit, Wärmeleitung und Tragfähigkeit im Falle eines Feuers widerstandsfähig sind. Neben der vorbeugenden Brandschutzfunktion zielt der bauliche Brandschutz auch auf die Vermeidung der Brand- und Rauchausbreitung ab. Dies wird durch die Bildung von Brandabschnitten sichergestellt. Die Bildung eines Brandabschnitts kann sowohl durch eine räumliche als auch durch eine bauliche Trennung realisiert werden.

Die räumliche Brandabschnittstrennung ist gegeben, wenn der Abstand zwischen Gebäuden bzw. Lägern mit nicht brennbaren Stoffen mindestens fünf Meter beträgt. Im Falle einer Lagerung von brennbaren Stoffen ist ein Mindestabstand von zwanzig Metern zwischen den Lagern zu wahren. Die Bildung von Brandabschnitten durch bauliche Maßnahmen ist durch den Einsatz von Brandwänden möglich. Brandwände sind solche Wände, die nach der Norm DIN 4102 die Feuerwiderstandsklasse F 90-A aufweisen und somit im Falle eines Brandes die Einwirkungen der Flammen, die Weiterleitung von Wärme sowie die Strahlung von Wärme durch Brandgase auf den dahinter liegenden Abschnitt für mindestens 90 Minuten verhindern. Die Brandschutzwand muss durch alle Stockwerke führen und darf nicht mit Öffnungen versehen sein. Sind Öffnungen aufgrund der betrieblichen Tätigkeit nicht vermeidbar, sind diese feuerbeständig zu schützen. Auch für diese Schutzmaßnahmen wie Verglasungen, Feuerschutzklappen etc. gilt eine Mindestwiderstandszeit von 90 Minuten. Darüber hinaus sind weitere Besonderheiten bei unterschiedlichen Gebäudehöhen oder im Winkel von weniger als 120 Grad zueinander stehenden Gebäuden und Lägern zu beachten (vgl. GDV 2018, S. 10 ff.).

Zur Verminderung des Feuerrisikos trägt darüber hinaus eine frühzeitige Brandentdeckung bei. Je früher ein Brand registriert und gemeldet wird, desto effizienter kann dieser bekämpft werden. Hieraus ergeben sich regelmäßig geringere Schadenausmaße. Häufig erfüllen Brandmeldeanlagen (BMA) noch weitere Funktionen und sorgen beispielsweise für das automatische Verschließen der Brandschutztüren oder das Abschalten der Klimaanlage, um Rauchverbreitungen zu vermeiden. Darüber hinaus ist auch der Meldeverlauf der BMA wesentlich für deren Effektivität. Hierbei sind drei grundsätzliche Verläufe zu unterscheiden. Der schnellste Weg ist die unmittelbare Aufschaltung der BMA an eine Feuerwehr. Weiter gibt es BMA, die den Alarm an eine Zwischenstelle melden, welche schließlich den Brand der Feuerwehr anzeigen. Hierbei wird zwischen Stellen unterschieden, die ständig und nicht ständig besetzt sind. Entsprechend kann es bei nicht ständig besetzten Stellen passieren, dass der Brand nicht an die Feuerwehr gemeldet wird (vgl. GDV 2008, S. 68 ff.).

Für Betriebe mit einer schlechten Anbindung zur Feuerwehr oder einer zu erwartenden schnellen Brandausbreitungsgeschwindigkeit, welche beispielsweise durch eine hohe bauliche Brandlast oder Brandlasten in Form von Maschinen, Vorräten, Betriebsmittel, Verpackungen etc. bedingt sein kann, sind ortsfeste automatische Feuerlöschanlagen empfehlenswert oder auch gesetzlich vorgeschrieben. Diese erkennen, melden und bekämpfen Brände unmittelbar (vgl. GDV 2008, S. 74). Hierbei sind diverse Arten von Löschanlagen zu unterscheiden: Wasserlöschanlagen, Schaumlöschanlagen, Pulver-Löschanlagen, Gaslöschanlagen, Inertgas-Löschanlagen, Raum-Inertisierungsanlagen, Aerosollöschanlagen oder Mehrstoff-Löschanlagen. Abhängig von den individuellen Gegebenheiten jedes einzelnen Betriebs ist zu überprüfen, welche Löschanlagen geeignet sind. Es wird empfohlen die hydraulischen Berechnungen für Löschanlagen sowie deren Installation ausschließlich durch VdS-anerkannte Firmen durchführen zu lassen. Darauf hinaus ist im Rahmen der technischen Maßnahmen eine ausreichende Wasserversorgung für die Brandbekämpfung sicherzustellen. Hierzu eignen sich Löschwasserentnahmestellen, wie innen- und außen liegende Hydranten oder Löschwasserteiche. Schließlich sind für feuergefährliche Stoffe sachgemäße Aufbewahrungsbehälter zu verwenden. Außerdem ist darauf zu achten, dass die Abstände im Rahmen der Brandabschnittsregelungen gewahrt werden, um im Falle eines Brandes ein Übergreifen des Feuers auf andere Abschnitte zu vermeiden. Entsprechend dürfen keine brennbaren Materialien in den Zwischenbereichen gelagert sein.

Versorgung

Um die Vulnerabilität gegenüber Versorgungsanfällen zu reduzieren, eignet sich die Bildung von Redundanzen. So können beispielsweise zusätzliche Einspeisepunkte im eigenen Stromnetz installiert werden. Weiter sind Notstromaggregate zu installieren. Zur Sicherung der Wasser- oder Gasversorgung können zum Beispiel Brunnen auf dem Betriebsgrundstück gebohrt oder andere Speicherformen errichtet werden (vgl. Keil 2019, S. 194).

Cyber

Mittels technischer Maßnahmen ist ein Grundschutz für die informationstechnologischen Systeme sowie die gespeicherten Daten sicherzustellen. Dies beginnt bereits bei der Zutrittskontrolle zum Betrieb. Die Zugangsberechtigung ist durch Schlüsselkarten oder Transponder abzufragen. Für besonders schützenswerte Räume, zu denen beispielsweise Serverräume zählen, sind zusätzliche technische Schutzmaßnahmen, wie Einzelberechtigungen, Einbruchmeldeanlagen etc. einzuführen. Darüber hinaus muss der Zugriff auf Computer des Betriebs stets mit einer Authentifizierung des Nutzers verbunden sein. Die Passwörter der Nutzer sind regelmäßig zu ändern. Innerhalb des IT-Systems sind Zugriffs kontrollen zu implementieren. Entsprechend der Tätigkeiten der Mitarbeitenden sind Zugangsberechtigungen auf festgelegte Datensätze zu formulieren. Der Export und Import von Daten ist stets zu kontrollieren. So sollten zum Beispiel E-Mails mit sensiblen Daten verschlüsselt verschickt werden. Das Einspielen von Daten über USB-Sticks sollte ausschließlich durch berechtigte Personen möglich sein, welche die Inhalte vorab auf schädliche Programme prüfen. Darüber hinaus sind laufend Kopien vom Datenstamm abzuspeichern. Für Schutzprogramme, wie Firewalls, Virenscanner etc. sind laufend Updates zu machen. Eine große Herausforderung der Cyber-Gefahren sind die hohen Veränderungs geschwindigkeiten. Softwareanpassungen, die Entdeckung neuer Sicherheitslücken sowie neu entwickelte schädliche Programme führen zu einer Dynamik, der Unternehmen mit einer funktionierenden Sicherheitsarchitektur sowie -organisation entgegenwirken müssen (vgl. Erichsen 2015, S. 248). Unmittelbar mit dem Verhalten der Mitarbeitenden verknüpfte Cyber-Gefahren, wie das Öffnen von Anhängen in E-Mails deren Sender nicht bekannt sind, sind laufend gegenüber den Mitarbeitenden zu kommunizieren und entsprechende Schulungen durchzuführen.

Einbruchs-/Zutrittsschutz

Neben dem digitalen Schutz ist auch der analoge Schutz vor Kriminellen notwendig. Dem unbefugten Zutritt durch Dritte ist sowohl mit mechanischen als auch elektronischen Sicherungstechniken entgegenzuwirken. Beim Einbruchschutz kommt es speziell auf die Widerstandsfähigkeit von Umzäunungen, Wänden, Decken und Dächern sowie Fassaden elementen, wie Türen und Fenstern, an. Unzureichende Sicherungen sind anzupassen. Bei Türen ist darauf zu achten, dass die Zusammenstellung von Türblatt und Türrahmen sowie Türbändern, Türschloss, Beschlügen, Schließblechen und eventuelle zusätzliche Sicherungsmaßnahmen aufeinander abgestimmt sind. Eine höhere Widerstandsfähigkeit wird durch Zusatzschlösser, stabilere Türbänder, qualitativ hochwertige Schlösser mit Schließzyllindern, Querriegeln sowie einbruchhemmenden Füllungen, Schließblechen und Türschildern erzielt (vgl. GDV 2014, S. 12). Ebenso ist bei Fenstern der Austausch durch vom VdS anerkannte einbruchhemmende Fenster empfehlenswert.

Insbesondere gefährdete Objekte sind zusätzlich durch elektrische Maßnahmen zu schützen. Hierzu zählen Einbruchmeldeanlagen, die so konzipiert sind, dass Einbrüche frühzeitig erkannt werden. Gewöhnliche Einbruchmeldeanlagen greifen hingegen erst, wenn die mechanischen Sicherheitsvorkehrungen bereits überwunden sind. Darüber

hinaus sorgen sichtbare Videoüberwachungen auf dem Gelände und im Betrieb dafür, dass die Attraktivität eines Einbruchs für Kriminelle schwindet. Zutrittskontrollen durch Codes oder Schlüsselkarten dienen ebenso der Diebstahl- und Vandalismusprävention (vgl. GDV 2014, S. 24 ff.). Abhängig von der Größe und Nutzungsart des Betriebsgeländes reichen die Sicherungsmaßnahmen an den Grundstücksgrenzen, in Form von Umzäunungen, sowie die Sicherungsmaßnahmen am Betriebsgebäude nicht aus. Gelegentlich fordern gesetzliche Vorgaben oder zollrechtliche Bestimmungen ganzheitliche Schutzstrategien zur Einhaltung des planmäßigen Betriebsablaufs. Hervorzuheben sind Anfälligekeiten bei offenen Produktionseinheiten, bei der offenen Lagerung von Waren und Gütern auf dem Betriebsgelände sowie sensible Infrastruktureinrichtungen. Bei solchen bedarf es eines Perimeterschutzsystems, also eines ganzheitlichen Konzepts aus technischen und organisatorischen Sicherungsmaßnahmen, welches das Betriebsgebäude, das Betriebsgelände sowie die unmittelbar angrenzende Umgebung umfasst (vgl. GDV 2012, S. 5).

8.5.3.2 Technische Maßnahmen

Auch mittels organisatorischer Maßnahmen lassen sich die Risiken für ein Unternehmen reduzieren.

Im Rahmen des Brandschutzes ist in Betrieben das Rauchen zu untersagen und separate Raucherbereiche einzuführen. Elektrokleingeräte des Betriebs und der Mitarbeitenden sind regelmäßig durch Fachkräfte auf die elektrische Sicherheit zu überprüfen und mittels Klebeschild zu dokumentieren. Auch für die elektrischen Anlagen sind regelmäßige Prüfungen durch zertifizierte Fachfirmen durchzuführen. Da insbesondere Kabeltunnel oder Kabeltrassen ein erhöhtes Feuerrisiko und ein damit einhergehendes Betriebsunterbrechungsrisiko aufweisen, ist der Zustand dieser ebenso laufend zu überprüfen. Trägerbahnen, Beschichtungen bzw. Isolierungen sind nachzubessern und Fremdkörper zwischen den Kabeln zu entfernen. Grundsätzlich gilt, dass Powerkabel stets oberhalb der Datenkabel anzubringen sind. In Industriever sicherungsverträgen handelt es sich üblicherweise um eine Obliegenheit des Versicherungsnehmers, diese Prüfungen einmal im Jahr durch eine vom VdS anerkannte Firma auszuführen. Um im Notfall einen störungsfreien Einsatz der Feuerwehr zu gewährleisten, sollte ein Feuerwehreinsatzplan gemäß DIN 14095 vorliegen und regelmäßige Begehung und Trainings mit der lokalen Feuerwehr durchgeführt werden. Darüber hinaus sind alle Einrichtungen der Brandmeldung, Brandbekämpfung sowie Löschwasserversorgung jährlich zu kontrollieren. Feuergefährliche Arbeiten, wie Schweißen, Löten und Brennschneiden, sollten innerhalb von Betrieben nur nach erfolgten Genehmigungen (Heißarbeitserlaubnissen) durchgeführt werden.

Allgemein ist im Rahmen des präventiven Schutzes beim Einsatz von Fremdfirmen stets eine Unterweisung dieser durchzuführen und entsprechend zu dokumentieren. Das unbefugte Betreten des Firmengeländes durch Dritte ist durch Zugangskontrollen zu vermeiden. Essenziell für den Unternehmenserfolg und das technische Risikomanagement sind gut qualifizierte Mitarbeitende. In diesem Zusammenhang ist dafür zu sorgen, dass regelmäßig Weiterbildungen des Personals stattfinden. Für Mitarbeitende, die altersbedingt in absehbarer Zeit ausscheiden, sind klare Übergangsregelungen festzulegen, damit

frühzeitig neue Mitarbeitende eingearbeitet werden, um einen Know-How-Verlust zu vermeiden (vgl. Hagebölling 2009b, S. 188 f.).

In Bezug auf den Herstellungsprozess sind die wichtigsten Maschinen, die Bottlenecks, zu identifizieren. Die wirtschaftlichen Folgen eines Ausfalls auf den Betrieb bzw. auf das gesamte Unternehmen sowie die Ausfallzeiten müssen identifiziert sein. Um Ausfallzeiten zu verkürzen, ist es sinnvoll für wichtige Maschinen Ersatzteile oder ganze Ersatzmaschinen vorzuhalten. Außerdem sollten Serviceverträge mit den Herstellern der Maschinen vorliegen, welche die Maschinen regelmäßig warten, inspizieren und im Schadenfall schnelle Reparaturen durchführen.

Trotz eines umfangreichen technischen Risikomanagements bleibt das Risiko einer Betriebsunterbrechung stets bestehen. Für den Eintritt einer solchen Betriebsunterbrechung können Betriebe vorab Maßnahmen und Verantwortlichkeiten klären, welche sich im Schadensfall mindernd auswirken. Zunächst ist ein Schaden- bzw. Notfallmanagement für Großschäden zu benennen und zu planen, sodass im Notfall auf transparente, vordefinierte Verantwortlichkeiten und Vorgehensweisen zurückgegriffen wird. Hierbei ist beispielsweise zu prüfen, ob unternehmensintern Produktionsprozesse auf andere Betriebe verlagert werden können. Alternativ können Verträge mit anderen Unternehmen geschlossen werden, sodass im Schadenfall eine gegenseitige Unterstützung bei der Produktionsverlagerung erfolgt. Darüber hinaus sind Pläne in Bezug auf die Kommunikation und das Verhalten gegenüber Stakeholdern aufzustellen (vgl. Hagebölling 2009b, S. 190 f.).

8.6 Lieferkettenunterbrechungen und die Relevanz der Betriebsunterbrechungsversicherung

Das Unternehmen, also der Auftraggeber des Lieferantenaudits, bezweckt mit dem Einsatz von Maßnahmen das anfängliche Bruttonrisiko eines Lieferantenausfalls auf ein verbleibendes, für das Unternehmen akzeptables Netto-Risiko, zu reduzieren. Dennoch besteht stets die Gefahr, dass Unternehmen Risiken unbewusst tragen, da bei der Risikoanalyse Risiken nicht identifiziert oder falsch bewertet wurden und daraus resultierend kein Einsatz adäquater Steuerungsmaßnahmen stattfindet. Darüber hinaus besteht trotz umfassender Maßnahmen beim Lieferanten stets das Risiko eines Lieferantenausfalls. Daher bietet die Versicherungswirtschaft Produkte, die den Risikotransfer einer Betriebsunterbrechung bedingt durch einen Lieferantenausfall ermöglichen.

Betriebsunterbrechungsversicherungen decken den Ertragsausfallschaden infolge einer Betriebsunterbrechung. Versichert gelten dabei die entgangenen Erträge, die als Deckungsbeitrag für die den entgangenen Gewinn und die im Falle einer Betriebsunterbrechung fortlaufenden Kosten dienen. Hinzu kommen Schadenminderungskosten und abhängig von den jeweiligen Vertragsarten und den zugrunde liegenden Bedingungen die sogenannten Mehrkosten. Hierbei kann es sich beispielsweise um zusätzliche Kosten durch die Anmietung neuer Hallen oder Gebäude, Vertragsstrafen, zusätzliche Löhne und Gehälter durch Überstunden oder zusätzliche Transportkosten für die Verlagerung von

Waren aus anderen Betriebsstandorten (vgl. Keil 2019, S. 105). Die Entschädigungspflicht des Versicherers ist auf die vertraglich vereinbarte Haftzeit begrenzt. Diese beträgt in der Regel zwölf bis 36 Monate. Überschreitet der Unterbrechungsschaden die Haftzeit, ist der Versicherer nicht zur Leistung der finanziellen Schäden, die nach der Haftzeit entstehen, verpflichtet. Die Haftzeit beginnt mit dem Sachschaden oder der Betriebsstörung, aus welcher die Betriebsunterbrechung resultiert. Die Entschädigungspflicht des Versicherers endet jedoch nicht mit der wieder hergestellten technischen Betriebsbereitschaft. Das Ende der Betriebsunterbrechung trifft vielmehr dann ein, wenn die vor Eintritt der Betriebsunterbrechung vorhandene Leistungsstärke auch in Bezug auf die Ertragskraft volumnfänglich erreicht ist (vgl. Philipp 2015, Rn. 171).

Für die Absicherung von Betriebsunterbrechungen durch Lieferantenausfälle lassen sich zwei wesentliche Deckungskonzepte unterscheiden. Zum einen können **gefährorientierte Deckungskonzepte** Versicherungsschutz bieten. Voraussetzung für die Entschädigung im Rahmen dieser ist der Eintritt eines Sachschadens. Der Sachschaden gilt als erfüllt, wenn eine dem Betrieb dienende Sache, bedingt durch eine versicherte Gefahr, zerstört oder beschädigt wird bzw. abhandenkommt. Zu unterscheiden sind die Feuer-Betriebsunterbrechungsversicherung, die Extended Coverage- und All Risk Betriebsunterbrechungsversicherung. Die einzelnen Gefahren dieser Deckungen werden in Tab. 8.2 abgebildet.

Im Rahmen der oben genannten Betriebsunterbrechungsversicherungen ist nicht nur die Betriebsunterbrechung durch eintretende Gefahren an eigenen Produktionsstandorten des Unternehmens versichert, sondern es lassen sich ebenso Betriebsunterbrechungen versichern, die durch den Ausfall von Zulieferern und Abnehmern begründet sind. Voraussetzung für den Versicherungsschutz ist, dass der Ausfall dieser Unternehmen ebenfalls durch den Eintritt eines Sachschadens, welcher sich durch eine versicherte Gefahr realisiert hat, bedingt ist. Die Betriebsunterbrechung infolge des Ausfalls eines externen Lieferanten oder Abnehmers wird als Rückwirkungsschaden bezeichnet. Gleichwohl bedarf es auch für die Mitversicherung der Rückwirkungsschäden durch Abnehmer oder Zulieferer der besonderen Vereinbarung. Für Rückwirkungsschäden sind üblicherweise Entschädigungs-grenzen vereinbart.

Tab. 8.2 Feuer-BU-Versicherung. Extended Coverage-BU. All Risk BU

- Brand	- Leitungswasser, Sturm/ Hagel, Einbruchdiebstahl	- Die Deckung umfasst sämtliche Gefahren, die zu einem Sachschaden und der daraus resultierenden Betriebsunterbrechung führen, es sei denn diese Gefahren werden explizit im Bedingungswerk ausgeschlossen.
- Blitzschlag	- Elementargefahren	
- Anprall oder Absturz eines Luftfahrzeugs, seiner Teiler oder seiner Ladung	- Gefahren, wie Fahrzeuganprall, Wasserlöschanlagen- leckage, Rauch, Überschalldruckwellen	
- Explosion und Implosion	- Innere Unruhen, Streik, Aussperrung, böswillige Beschädigungen	

Andererseits gibt es auch die sogenannten *Supply-Chain-Policen*. Bei diesen Policen bedarf es für den Eintritt des Versicherungsfalls keinen vorangegangenen Sachschaden. Die Haftzeit beginnt mit dem Lieferausfall. Insofern unterscheidet sich die Supply-Chain-Police stark von der zuvor genannten Deckung für Rückwirkungsschäden. Derartige Policen werden jedoch nur von wenigen Risikoträgern angeboten und sind darüber hinaus mit hohen Prämien verbunden. Die Prämiensätze liegen bei ca. drei bis vier Prozent, so dass sich bei einer relativ geringen Deckungssumme von 1.000.000 Euro bereits eine Jahresprämie in Höhe von 30.000 bis 40.000 Euro ergibt (vgl. Keil 2019, S. 201 f.).

Ein Unternehmen zielt mit dem Abschluss einer Versicherung letztlich darauf ab, das individuelle Risiko auf ein akzeptables Maß zu reduzieren. Da Versicherungen jedoch nur die letzte Verteidigungsline bilden, ist ein umfassendes technisches Risikomanagement innerhalb von Unternehmen unabdingbar.

Literatur

- Austrian Standards. (Hrsg.). (2014). Serie ONR 49000 – Risikomanagement für Organisationen und Systeme. Fachinformation 06. https://www.austrian-standards.at/dokumente/produkteloesungen/kostenlose-services/fachinformationen/06-risikomanagement/fachinformation06_risikomanagement.pdf. Zugegriffen am 01.09.2020.
- Brühwiler, B., & Romeike, F. (2010). *Praxisleitfaden Risikomanagement: ISO 31000 und ONR 49000 sicher anwenden*. Berlin: Erich Schmidt.
- Diedrichs, M. (2018). *Risikomanagement und Risikocontrolling* (4. Aufl.). München: Fanz Vahlen.
- DIN (Hrsg.). (2015). DIN ISO 9000:2015-12, *Qualitätsmanagementsysteme – Grundlagen und Begriffe*. Berlin: Beuth.
- DIN (Hrsg.). (2018). *DIN ISO 31000:2018-10, Risikomanagement – Leitlinien*. Berlin: Beuth.
- Erichsen, S. (2015). Cyber-Risiken und Cyber-Versicherung: Abgrenzung und/oder Ergänzung zu anderen Versicherungssparten. *CCZ – Corporate Compliance*, 6, 247–250.
- FM Global. (Hrsg.) (2016). Property Loss Prevention Data Sheets – Flood. <https://www.fmglobal.com/-/media/Documentum/Data-Sheet-Individual/01-Construction/FMDS0140.pdf?isGated=true&itemId={66786966-6C7F-4EA9-B163-933C24E81511}>. Zugegriffen am 30.07.2019.
- GDV (Hrsg.). (2008). *Technischer Leitfaden der Feuer- und Feuerbetriebsunterbrechungs-Versicherung – Risiken, Schutzziele, Schutzkonzepte und Schutzmaßnahmen*. Köln: VDS Schadenverhütung GmbH.
- GDV (Hrsg.). (2012). *Sicherungsleitfaden – Perimeter*. Köln: VDS Schadenverhütung GmbH.
- GDV (Hrsg.). (2014). *Sicherungsrichtlinien für Geschäfte und Betriebe*. Köln: VDS Schadenverhütung GmbH.
- GDV (Hrsg.). (2016). *Schutz vor Sturm*. Köln: VDS Schadenverhütung GmbH.
- GDV (Hrsg.). (2018). *Brand- und Komplex trennwände – Merkblatt für die Anordnung und Ausführung*. Köln: VdS Schadenverhütung GmbH.
- Gietl, G., & Lobinger, W. (2016). *Leitfaden für Qualitätsaudитoren – Planung und Durchführung von Audits nach ISO 9001:2015* (5. Aufl.). München: Hanser.
- Glage, D., & Grötzner, M. (2016). § 14 Unternehmensrisiken und Risikomanagement. In Hauseck, Moosmayer & Lösler (Hrsg.), *Corporate Compliance – Handbuch der Haftungsvermeidung im Unternehmen* (3. Aufl.). München: C. H. Beck.
- Hagebölling, V. (2009a). Technisches Risikomanagement. In V. Hagebölling (Hrsg.), *Technisches Risikomanagement. Leitfaden für die Praxis* (1. Aufl., S. 32–45). Köln: TÜV Media GmbH TÜV Rheinland GmbH.

- Hagebölling, V. (2009b). Anhang – Checklisten. In V. Hagebölling (Hrsg.), *Technisches Risikomanagement. Leitfaden für die Praxis* (1. Aufl., S. 46–30). Köln: TÜV Media GmbH TÜV Rheinland GmbH.
- Hommelhoff, P., & Mattheus, D. (2000). Gesetzliche Grundlagen: Deutschland und international. In Dörner et al. (Hrsg.), *Praxis des Risikomanagements. Grundlagen, Kategorien, branchenspezifische und strukturelle Aspekte* (S. 5–40). Stuttgart: Schäffer-Poeschel.
- Jörgl, T. (2009). Dem Feuer die Luft nehmen. *Lististik Heute*, 11, 54–57.
- Kaiser, S. (2016). Ölkatstrophe kostet laut BP knapp 62 Milliarden Dollar. In *Spiegel Online*. <https://www.spiegel.de/wirtschaft/unternehmen/deepwater-horizon-bp-beziffert-kosten-auf-62-milliarden-dollar-a-1103100.html>. Zugegriffen am 12.08.2019.
- Keil, R. (2019). *Betriebsunterbrechungsversicherung – Ursachen, Wirkungen und Lösungen*. Karlsruhe: VVW GmbH.
- Philipp, P. (2015). § 31. Feuerversicherung, Feuerbetriebsunterbrechungsversicherung. In Beckmann & Matuschke-Beckmann (Hrsg.), *Versicherungsrechts-Handbuch* (3. Aufl.). München: C. H. Beck.
- Preiss, R. (2017). *Methoden der Risikoanalyse in der Technik – Systematische Analyse komplexer Systeme* (2. Aufl.). Wien: TÜV Austria Akademie GmbH.
- Rohlf, T. (2018). *Risikomanagement im Versicherungsunternehmen – Identifizierung, Bewertung und Steuerung* (2. Aufl.). Karlsruhe: VVW.
- Schlatt, A. (2016). Single Sourcing – der hohe Preis der Abhängigkeit. In Produktion, Materialwirtschaft & Logistik | Genios WirtschaftsWissen, Nr. 09 vom 26.09.2016. http://www.genios.de/wirtschaft/single_sourcing_der_hohe_preis_der_abh/c_produktion_20160926.html. Zugegriffen am 15.05.2019.
- Schnorrenberg, U., & Goebels, G. (1997). *Risikomanagement in Projekten – Methoden und ihre praktische Anwendung*. Braunschweig/Wiesbaden: Vieweg.
- Wagner, F. (2000). *Risk Management – im Erstversicherungsunternehmen*. Karlsruhe: VVW.
- Zentis, T. (2013). Modell zur Bewertung und Kontrolle technischer Risiken. In F. Klocke et al. (Hrsg.), *Ergebnisse aus der Produktionstechnik. Band 22/2013*. Aachen: Apprimus.
- Zentis, T., et al. (2011). *Technisches Risikomanagement in produzierenden Unternehmen*. Aachen: Apprimus.
- Zentis, T. et al. (2012). Durch technisches Risikomanagement den Unternehmenserfolg absichern. In *ZWF, Jahrgang 107*, München: Carl Hanser, S. 256–260.

Thomas Bär studierte Schiffsbetriebstechnik an der TU Rostock, Abschluß Dipl. Ing. und Lizenz: CI, Chief Engineer Officer auf Großschiffen mit unlimitierter Antriebsleistung. Mehr als 15 Jahre tätig als Chief Engineer und technischer Flottenmanager und war verantwortlich für das technische und personelle Management von Großschiffen. Seit 1994 in verschiedenen Führungspositionen bei international agierenden Industriever sicherern, verantwortlich für die Betreuung und risikotechnische Beratung von multinationalen Großunternehmen. Gründung der „Bär Consulting“ in 2017. Bär Consulting analysiert und quantifiziert interne und externe Risiken in Industrieunternehmen und bei deren Lieferanten bzw. Kunden. BC entwickelt individuelle und praktikable Vorschläge, um kritische Risiken auf ein für das individuelle Unternehmen akzeptable Maß zu senken – weltweit.

Yannick Berkemeier absolvierte am ivwKöln den Bachelorstudiengang Versicherungswesen mit den Schwerpunkten Haftpflicht-/Unfall-/Kraftfahrt-/Rechtsschutzversicherung, Sach- und Betriebs unterbrechungsversicherung sowie Personalwesen. Anschließend setzte er seine Ausbildung mit dem Masterstudiengang Risk & Insurance am ivwKöln fort. Insbesondere in der Maklertätigkeit für Gewerbe und Industrikunden hat er seit Beginn des Studiums bei der Ecclesia Gruppe Erfahrungen gesammelt. Am Standort Köln ist er verantwortlich für die Absicherung von Cyber-Risiken.



Schaden- und Krisenmanagement

9

Michael Seidl und Kathrin Regeling

Zusammenfassung

Das Schaden- und Krisenmanagement beschäftigt sich mit der Prävention sowie Bewältigung von Schäden und Krisen. Dem Krisenmanagement ist ein Schaden oder Ereignis zuzuordnen, welcher/welches zu einer ernsthaften bis hin zu einer existenzbedrohliche Lage für das Unternehmen führen kann. Dementsprechend sind Schaden- und Krisenmanagement eng miteinander verflochten. Hierbei ist insbesondere darauf hinzuweisen, dass eingetretene Schäden ohne strukturierte Methoden zur Bewältigung häufig das Potenzial besitzen, sich zu einer Krise auszuweiten. Allein die Entstehung einer öffentlichen Meinung, ein Unternehmen habe im Schadenfall nicht oder falsch reagiert, kann für dieses Unternehmen bereits zu einer Krise führen. Je nach Risiko sind unterschiedliche Maßnahmen im Rahmen des Schaden- und Krisenmanagements erforderlich.

9.1 Einleitung

Für den Erfolg eines Unternehmens ist nicht nur die Qualität der angebotenen Produkte und Dienstleistungen entscheidend, sondern auch der Umgang mit außergewöhnlichen und bedrohlichen Situationen. Die üblichen Betriebsabläufe können gestört werden, was dazu führen könnte, dass Stakeholder beunruhigt werden und die Öffentlichkeit das Ver-

M. Seidl (✉)

DMW Assekuranz und Risikomanagement GmbH, Geisenhausen, Deutschland
E-Mail: michael.seidl@dmw-assekuranz.de

K. Regeling

TH Köln, Institut für Versicherungswesen, Köln, Deutschland
E-Mail: Regeling.Kathrin@gmail.com

trauen verliert. Diesen Risiken muss sich ein Unternehmen stellen und Vorkehrungen treffen. Ein wirkungsvolles, strategisches Instrument diesen Risiken zu begegnen ist die Implementierung eines Schaden- und Krisenmanagements.

Im Folgenden wird einleitend darauf eingegangen, wie das Schaden- und Krisenmanagement definiert ist, was man unter einer Krise versteht, welche begrifflichen Abgrenzungen beachtet werden sollten und welche Merkmale und Phasen eine Krise hat. Ein Unternehmen ist von vielseitigen Risiken bedroht, welche zu Schäden oder sogar zu Krisen führen können. Das Schaden- und Krisenmanagement, als Teil des Risikomanagements, sind in erster Linie auf die Vermeidung speziell von Schäden auszurichten. Da die gänzliche Vermeidung von Schäden jedoch reine Utopie ist, muss insbesondere das Schadenmanagement auch ausreichend strukturiert auf die Mitigation bereits eingetretener Schäden reagieren. Das Schadenmanagement teilt sich dabei auf in Schadenprävention und Schadenbewältigung. Das Krisenmanagement ist im Prinzip ähnlich wie das Schadenmanagement aufgeteilt – und zwar in Krisenprävention und Krisenbewältigung. Zudem wird das Schaden- und Krisenmanagement anhand des Risikos für die Mitarbeitersicherheit dargestellt. Im Fazit werden die bedeutendsten Aspekte zusammengefasst.

9.2 Definition und Zielsetzung des Schaden- und Krisenmanagements

Das Risikomanagement ist dem Krisenmanagement übergeordnet (vgl. Brühl et al. 2018, S. 5) und beschäftigt sich laufend mit der Handhabung sämtlicher unternehmerischer Risiken (vgl. Martin und Bär 2002, S. 28). Im Rahmen des Risikomanagements gilt es, diese zu vermeiden, vermindern, transferieren und selbst zu tragen (vgl. Rohlfs 2018, S. 74). Kommt es zu der außerordentlichen Situation, dass ein solches Risiko nicht vermieden wird (oder vermieden werden kann) und sich zu einer Krise entwickelt, so ist das Krisenmanagement betroffen (vgl. Martin und Bär 2002, S. 28). Somit wird das Krisenmanagement nicht isoliert, sondern als Teil des Risikomanagements betrachtet (vgl. Brühl et al. 2018, S. 5).

Bislang gibt es keine einheitliche Definition des Krisenmanagements. Daher fehlt es auch an einer allgemeingültigen Bezeichnung der Krisenmanagement-Bestandteile. Zum besseren Verständnis werden dafür in dieser Arbeit die Begriffe „Krisenprävention“ und „Krisenbewältigung“ verwendet. Die von Krystek verwendete Bezeichnung „Krisenvermeidung“ sowie die Begriffe „Krisenvorsorge“ und „aktives Krisenmanagement“ werden im Folgenden unter „Krisenprävention“ vereint. „Akutes Krisenmanagement“ wird in dieser Darstellung als „Krisenbewältigung“ bezeichnet.

Gegenstand jeder Definition ist die Krisenbewältigung. Im weiteren Sinne, wird auch die Krisenprävention mit einbezogen. Gemäß der Definition nach Müller wird unter dem Krisenmanagement lediglich die Krisenbewältigung verstanden. Krystek legt den Begriff weiter aus und bindet ebenfalls die Krisenprävention mit ein (vgl. Martin und Bär 2002, S. 27). Seiner Definition nach, sind bereits vor Eintritt der Krise besondere Strategien er-

forderlich, die dabei helfen, dass es nicht zu einer Krise kommt. Sie sind somit der Krisenprävention bzw. dem Krisenmanagement zuzuordnen (vgl. Brühl et al. 2018, S. 29). Der Definition von Krystek ist hier gegenüber der von Müller der Vorzug zu geben, da der Fokus nach Möglichkeit immer zuerst auf das Erkennen und die Vermeidung einer problematischen Situation gelegt werden sollte. Gemäß seiner Definition wird die Existenzsicherung des Unternehmens als Ziel des Krisenmanagements nicht allein durch die Krisenbewältigung, sondern auch durch die Krisenprävention erreicht. Im Rahmen der Existenzsicherung könnte im weitesten Sinne jede Unternehmensaktivität verstanden werden, die der Realisierung von Unternehmenszielen dient.

Mit dem Hintergrund, dass Schäden Auslöser einer Krise sein können und/ oder eine Krise einen Schaden zur Folge hat, besteht zwischen dem Schaden- und Krisenmanagement eine enge Verknüpfung. Dementsprechend gehört zur Implementierung eines Krisenmanagements die des Schadenmanagements und umgekehrt. Aufgrund der starken Verflechtung beider Bereiche, ist die Existenz des einen ohne das andere nicht möglich. Zum Schadenmanagement zählen somit die Schadenprävention sowie die Schadenbewältigung. Das primäre Ziel der Schadenprävention ist es, die Eintrittswahrscheinlichkeit eines Schadens zu minimieren. Im Rahmen der Schadenbewältigung sollen Maßnahmen ergriffen werden, um den bereits eingetretenen Schaden zu steuern, dessen Folgen zu mindern und den Normalbetrieb des Unternehmens wieder sicher zu stellen (Schadenbewältigung).

Das Schaden- und Krisenmanagement wird vom Risikomanagement gesteuert. Das Risikomanagement dient dabei als Grundlage für das strukturierte und prozessorientierte Erarbeiten von Vermeidungs- und Bewältigungsstrategien durch das Schaden- und Krisenmanagement.

9.2.1 Definition einer Krise

Der Begriff „Krise“ stammt aus dem Griechischen und wurde aus dem Wort „Krísi“ abgeleitet. Die ursprüngliche Definition hat ihre Wurzeln im medizinischen Bereich und beschreibt den Verlauf einer Krankheit, welche entweder zu ihrem Höhepunkt, dem Tod oder zu einem Wendepunkt, der Genesung, führt. Im Laufe der Zeit wurde diese Definition auf weitere Wissenschaftsdisziplinen übertragen (vgl. Sieg 1999, S. 2). In den Wirtschaftswissenschaften wird unter einer Krise im Allgemeinen ein Ereignis oder eine Störung, welches/ welche die Rentabilität und Reputation eines Unternehmens auf längere Dauer nachteilig beeinflussen könnte, verstanden (= Unternehmenskrise) (vgl. Höbel und Hofmann 2013, S. 12). Im Folgenden wird näher auf die Unternehmenskrise eingegangen, von der in der Literatur jedoch keine einheitliche Definition zu finden ist (vgl. Sieg 1999 S. 2). Eine ausführliche Definition stammt von Krystek: „Unternehmenskrisen sind ungeplante und ungewollte Prozesse von begrenzter Dauer und Beeinflussbarkeit sowie mit ambivalentem Ausgang. Sie sind in der Lage den Fortbestand der gesamten Unternehmung substantiell und nachhaltig zu gefährden oder sogar unmöglich zu machen. Dies geschieht

durch die Beeinträchtigung dominanter Ziele, deren Gefährdung oder gar Nichterreichung gleichbedeutend ist mit einer nachhaltigen Existenzgefährdung oder Existenzvernichtung der Unternehmung als selbstständig und aktiv am Wirtschaftsprozess teilnehmender Einheit mit ihren bis dahin gültigen Zweck- und Zielsetzungen.“ (Krystek 1987, S. 6). Zusammengefasst ist eine Unternehmenskrise ein Risiko der Nichterreichung des übergeordneten Ziels der langfristigen Sicherung der Unternehmensexistenz und des Unternehmenserfolgs. Aus Sicht der Praxis ist die Definition von Krystek jedoch zu weitgehend, da eine Krise zwar eine außergewöhnliche Situation für das Unternehmen darstellt und in der Lage ist, zu einer Existenzbedrohung zu führen, aber nicht zwangsläufig mit einer verbunden sein muss. Jedes Unternehmen kann, unabhängig von der Definition nach Krystek, selber festlegen ab wann es von einer Krise spricht und wie es diese definiert. So kann eine Krise bereits vorliegen, wenn das Eintreten einer außergewöhnlichen Situation dafür sorgt, dass das Unternehmen bestimmte vereinbarte Ziele nicht erreichen kann. Eine ernsthafte Bedrohung dieser Ziele kann ausreichen, um als Krise zu gelten. Es muss daher nicht zwangsläufig eine Existenzbedrohung mit der Krise einhergehen.

Eine Krise kann sowohl das ganze Unternehmen betreffen, als auch einen begrenzten lokalen Einfluss haben. Ebenso kann eine Krise intern oder extern auftreten. Führt ein Erdbeben in Japan dazu, dass eine Produktionshalle eines international tätigen Unternehmens einstürzt und daher für eine gewisse Zeit nicht produziert werden kann, kann dies zu einer lokalen Krise führen. Diese muss nicht zwangsläufig auf das gesamte Unternehmen übergreifen. Die Krise könnte lokal eingegrenzt werden, soweit es gelingt, zum Beispiel auf vorher im Krisenplan festgelegte Alternativen zurückzugreifen, um die Produkte dort zu produzieren, wie zum Beispiel einer Produktionsverlagerung innerhalb der Unternehmensgruppe oder der Zugriff auf externe Kapazitäten. Gelingt dies nicht und werden auch andere Standorte des Unternehmens durch die Krise in Japan nachteilig beeinflusst, könnte dies zu einer Krise für das gesamte Unternehmen und somit zu einer Existenzbedrohung führen.

Erdbeben oder sonstige Naturkatastrophen sind typische Beispiele für externe Risiken. Auch geänderte gesetzliche Regelungen, Kampagnen, Sabotagen können das Unternehmen treffen. Insbesondere aber auch die stark zunehmende Digitalisierung führt zu großem Risikopotenzial wie zum Beispiel Cyberattacken.

Interne Krisen dagegen haben ihre Ursache, im eigentlichen Betrieb. Beispiele dafür sind Unterschlagung und Korruption, Produktmängel- oder Rückrufe sowie Störfälle oder Arbeitsunfälle.

Wie bereits beschrieben, kann eine Unternehmenskrise ihren Ursprung in unterschiedlichen Risiken haben. Die Risiken eines Beispielunternehmens können folgende sein:

- Risiken für die Mitarbeitersicherheit: Den Arbeitgeber trifft in Deutschland eine Fürsorgepflicht gegenüber seinen Arbeitnehmern gemäß §§ 241 Abs. 2 und 618 BGB. Er ist jedoch nicht nur in rechtlicher, sondern auch moralischer Hinsicht verpflichtet, das Leben und die Gesundheit der Mitarbeiter zu schützen. Wird das Leben oder die Gesundheit eines Mitarbeiters zum Beispiel durch Terroranschläge, Naturkatastrophen

oder Entführungen gefährdet, könnte dies hohe Reputationsschäden nach sich ziehen (vgl. Schaefer und General Manager Central Europe der International SOS 2012, S. 21).

- IT-Risiken/Cyber-Risiken: Da die Gesellschaft immer digitaler wird und damit die Bedrohung durch Cyber-Risiken stärker wächst, sollte sich ein Unternehmen darauf vorbereiten und entsprechende Vorsorge treffen (vgl. Hustedt 2019, S. 1). IT-Risiken können extern zum Beispiel durch Hackerangriffe entstehen. Intern können sie entstehen, wenn zum Beispiel ein Mitarbeiter eine unsichere Software installiert.
- Naturkatastrophen/Brandkatastrophen: Naturkatastrophen können dazu führen, dass Produktionsstätten beschädigt/zerstört werden oder Mitarbeiter verletzt/getötet werden. Naturgefahren sind zum Beispiel Erdbeben, Vulkanausbruch, Orkane, Stürme, Feuer, Tsunami und Überschwemmungen. Naturkatastrophen und Feuer sind eine der häufigsten Ursachen für Betriebsunterbrechungen (vgl. Thießen 2014, S. 291).
- Wirtschaftliche Risiken/Betriebsunterbrechung: Kommt es in einer Produktionsstätte zu einem Sachschaden und erleidet das Unternehmen einen Ertragsausfall, sofern zeitweise nichts mehr produziert werden kann, kommt es zu einem Betriebsunterbrechungsschaden, welcher in der Lage sein kann, eine Krise auszulösen.
- Strafrechtliche und wettbewerbsrechtliche Risiken: Strafrechtliche Risiken können Unternehmen betreffen, wenn zum Beispiel durch ihre vertriebenen Produkte eine Person einen Schaden erleidet und daraufhin ein strafrechtliches Ermittlungsverfahren eingeleitet wird. Wettbewerbsrechtliche Risiken kommen beispielsweise vor, wenn ein Unternehmen gegen Patentvorschriften verstößt. Dies kann zu einer Krise heranwachsen, wenn das Produkt bereits in den Markt gebracht wurde und die weitere Produktion aufgrund des Verstoßes abgebrochen werden muss.
- Haftpflichtrisiken: Haftpflichtrisiken von Unternehmen liegen zum Beispiel vor, wenn ein mangelhaftes Produkt auf den Markt gebracht wird und daraufhin behördliche Rückrufaktionen sowie Personenschäden drohen.

9.2.2 Begriffliche Abgrenzungen

Für den Begriff „Krise“, werden in der Umgangssprache häufig verschiedene Bezeichnungen synonym verwendet. Es handelt sich dabei unter anderem um die Begriffe „Risiko“, „Notfall“ und „Katastrophe“. Diese Bezeichnungen sind inhaltlich von der Krise zu unterscheiden:

- Risiko und Krise: Risiken können dazu führen, dass die Erreichung von Zielen (zum Beispiel Gewinnziele, Wachstumsziele) gefährdet wird. Diese sind dem obersten Ziel, der Existenzsicherung, untergeordnet. Ein Risiko, welches sich derart entwickelt, dass es die Existenz des Unternehmens bedroht, nennt man Unternehmenskrise (vgl. Martin und Bär 2002, S. 28).
- Notfall und Krise: Obwohl die Begriffe Krise und Notfall in der Umgangssprache teilweise synonym verwendet werden, sind sie voneinander abzugrenzen. Unter einem

Notfall wird ein Ereignis verstanden, welches plötzlich eintritt und bei fehlendem Handeln das Potenzial besitzt, die Existenz des betroffenen Unternehmens zu bedrohen. Im Rahmen des Notfallmanagements steht bei der Schadenbewältigung ein schnelles und effektives Handeln im Vordergrund, welches dazu dienen soll, die Not abzuwenden. Eine Krise entwickelt sich (unter Umständen „schleichend“) über die Zeit und stellt einen Wendepunkt vom positiven zum negativen Geschehen dar. Beim Krisenmanagement hingegen ist (im Gegensatz zum Notfallmanagement) weniger ein schnelles, wirksames Handeln von Bedeutung, sondern das Treffen von Entscheidungen (vgl. Brauner 2001, S. 13).

- Katastrophe und Krise: Unter einer Katastrophe wird eine Unternehmenskrise verstanden, die nicht vermeidbar ist und welche das Unternehmen nicht überstehen wird. Im Gegensatz dazu, ist bei einer Unternehmenskrise die Weiterführung des Unternehmens zwar gefährdet, aber nicht zwangsläufig mit einer Insolvenz des Unternehmens verbunden. Die Krise erschwert in der Regel jedoch die Zielsetzung des Unternehmens (vgl. Thießen 2014, S. 32).

9.2.3 Merkmale einer Krise

Trotz der Einzigartigkeit einer jeden Krise, lassen sich die in Abb. 9.1 dargestellten gemeinsamen Merkmale feststellen.



Abb. 9.1 Merkmale einer Krise. (Quelle: eigene Darstellung in Anlehnung an Thießen 2014, S. 31)

Die Merkmale einer Krise werden im Folgenden anhand eines möglichen Praxisbeispiels beschrieben:

Ein Lebensmittelhersteller vertreibt Babynahrung. 50 Säuglinge in Deutschland erkrankten nach der Aufnahme der Babynahrung mit der Geschmacksrichtung „Birne-Banane“. Es stellte sich heraus, dass sich Schadstoffe in der Nahrung befanden. Etliche Fälle, in denen Säuglinge, welche mit der Nahrung des besagten Lebensmittelherstellers gefüttert wurden und erkrankten, wurden schlagartig durch Zeitung und Fernsehen bekannt (ungeplant). Der Lebensmittelhersteller rief daraufhin alle Gläser der Geschmacksrichtung „Birne-Banane“ zurück. Der Hersteller versicherte, dass er regelmäßig die Babynahrung überprüft und dabei bisher keine Schadstoffe entdeckt wurden. Daher traf ihn die Krise plötzlich (unvorhersehbar). Aufgrund der schnellen Verbreitung durch die Presse nahm ein Großteil der Verbraucher Kenntnis von dem Vorfall (aufsehenerregend). Aufgrund des großen Vertrauensverlustes in die Marke bzw. den Lebensmittelhersteller gingen die Verkaufszahlen der Babynahrung zurück. Verbraucher mieden die Produkte und der Handel reagierte mit der Entfernung der Produkte aus den Regalen. Auch der Unternehmenswert sank drastisch, aufgrund des abgefallenen Aktienkurses (dynamisch). Die Kosten für die Rückrufaktion, waren, gemessen am Umsatz, relativ hoch. Zusätzlich mussten den Familien der betroffenen Säuglinge Schadenersatz gezahlt werden. Der angefallene Gesamtschaden, der sich aus dem Schadenersatz, den Kosten der Rückrufaktion, dem Nachfragerückgang, der Senkung des Unternehmenswertes und des Imageverlusts ergab, führte zur einer erheblichen finanziellen Belastung des Unternehmens und hätte potenziell eine Insolvenz herbeiführen können (existenzbedrohend).

9.2.4 Phasen einer Krise

Bisher bietet die Theorie kein einheitliches Krisenverlaufsmodell. In der Literatur wird der Krisenverlauf unterschiedlich dargestellt. Die Unterteilung des Krisenverlaufs ist von praktischer Bedeutung, da je nach Phase spezifische Maßnahmen erforderlich sind. Im Folgenden werden der jeweilige Krisenprozess nach Müller und Krystek dargestellt. Es handelt sich hier jeweils um Vier-Phasenmodelle, die auch inhaltlich teilweise übereinstimmen (vgl. Evertz und Krystek 2014, S. 7). Die Entwicklung der verschiedenen Krisenphasen nach Krystek und Müller ist abhängig davon, ob es sich um eine schleichende oder plötzliche Krise handelt (vgl. Thießen 2014, S. 242).

Krystek betrachtet den Krisenverlauf aus der Wahrnehmungsperspektive und beschreibt dazu folgende vier Krisenphasen (vgl. Thierhoff und Müller 2016, S. 23):

- Phase 1: Potenzielle Krise
- Phase 2: Latente Krise
- Phase 3: Akut/Beherrschbare Krise
- Phase 4: Akut/Nicht Beherrschbare Krise

Nach Krystek beginnt der Krisenverlauf mit der potenzielle Krise (Phase 1). Dass sich das Unternehmen bereits in einer anfänglichen Krise befindet, ist in dieser Phase jedoch noch nicht erkennbar. Eine Wahrnehmbarkeit der Krisenanzeichen liegt zu dem Zeitpunkt noch nicht vor (vgl. Evertz und Krystek 2014, S. 7). Das Unternehmen befindet sich in einem sogenannten „Quasnormalzustand“ (vgl. Thierhoff und Müller 2016, S. 24). An die potenzielle schließt sich die latente Krise (Phase 2) an, welche erst mithilfe der Anwendung von Früherkennungssystemen aufgedeckt werden kann. Entfällt der Einsatz dieser Systeme, bleibt die latente Krise unentdeckt. Sie wird somit nicht abgewehrt und führt zu einer akut/beherrschbaren Krise (Phase 3) (vgl. Evertz und Krystek 2014, S. 7). In dieser Phase besteht unter hohem Zeitdruck noch die Möglichkeit, die Krise zu bewältigen, sofern entsprechende komplexe Maßnahmen angewendet werden (vgl. Thießen 2014, S. 244). Das Vorliegen einer Krise ist deutlich sichtbar. Das Unternehmen ist mit der Krisenbewältigung überfordert. Gelingt die Beherrschung der Krise nicht, führt dies zur akut/nicht beherrschbaren Krise (Phase 4), welche ein Ausscheiden des Unternehmens (in bisheriger Substanz) aus dem Markt zur Folge hat (vgl. Evertz und Krystek 2014, S. 7).

Müller betrachtet die Krise aus der finanz- und erfolgswirtschaftlichen Perspektive. Unterteilt wird der Krisenverlauf ebenfalls in vier Phasen (vgl. Thierhoff und Müller 2016, S. 25):

- Phase 1: Strategiekrisse
- Phase 2: Erfolgskrise
- Phase 3: Liquiditätskrise
- Phase 4: Insolvenz

Der Krisenverlauf nach Müller zeigt die Abhängigkeit der Gefährdung der Erreichung der Unternehmensziele von der Zeit. Je weiter fortgeschritten die Krise ist, desto geringer wird der Handlungsspielraum zur Krisenbewältigung (vgl. Thierhoff und Müller 2016, S. 25). Müller gibt in seinem Modell einen Überblick über die Höhe der Anforderungen an die Maßnahmen der Krisenprävention oder -bewältigung in Abhängigkeit von der zeitlichen Entwicklung des Krisenverlaufs (vgl. Thießen 2014, S. 41).

Der Krisenverlauf nach Müller beginnt mit der sogenannten „Strategiekrisse“ (Phase 1). Durch falsche oder fehlende strategische Entscheidungen wird bereits in dieser Phase der Grundstein für die weitere Entwicklung der Krise gelegt. Auch das Fehlen einer Strategie kann zu einer solchen Krise führen. Diese frühe Art der Krise ist beispielsweise gekennzeichnet durch eine zunehmende Anzahl von Kundenbeschwerden, einem Nachfragerückgang oder einer Unzufriedenheit seitens der Mitarbeiter. In dieser Phase ist der Handlungsspielraum, die Krise abzuwenden noch groß. Werden keine Änderungen der Strategie vorgenommen oder der Fehler behoben, folgt die Erfolgskrise, bei der die Möglichkeit des Handelns minimiert wird (Phase 2) (vgl. Thießen 2014, S. 41). Während dieser Phase ist die Erreichung von Erfolgszielen, die zum Beispiel den Gewinn, die Rentabilität oder den Umsatz des Unternehmens betreffen, bedroht. Wird der Erfolgskrise langfristig nicht entgegengewirkt, schließt die Liquiditätskrise (Phase 3) an (vgl. Evertz und Krystek 2014,

S. 7). Das Unternehmen ist der Gefahr von ernsthaften Liquiditätsengpässen ausgesetzt (vgl. Thießen 2014, S. 41). In dieser Phase sind die Auswirkungen der Krise schon deutlich zu erkennen, denn das Unternehmen wird mit negativen Reaktionen seitens der Stakeholder konfrontiert. Beispielsweise liefern Lieferanten nur noch gegen Vorkasse (vgl. Thierhoff und Müller 2016, S. 25). Wird auch diese Bedrohung nicht bzw. nicht erfolgreich abgewendet, folgt die Insolvenz (Phase 4) als letzte Phase des Krisenverlaufs (vgl. Thießen 2014, S. 41).

Nicht jede Krise muss nach den oben dargestellten Modellen verlaufen. Möglich ist auch, dass Krisenphasen übersprungen werden oder sich die Krisenphasen nicht weiter – sondern zurückentwickeln (vgl. Thierhoff und Müller 2016, S. 25). Müller gibt beispielsweise an, dass eine Krise zwar in den meisten Fällen mit der strategischen Krise beginnt, es aber aus seiner Sicht die Möglichkeit des Einstiegs mit der Erfolgs- oder Liquiditätskrise gibt (vgl. Pastors 2002, S. 92). Dies kann der Fall sein, wenn geeignete Maßnahmen zur Abwehr der Krise angewandt werden (vgl. Thierhoff und Müller 2016, S. 25).

Die beiden dargestellten Phasen des Krisenverlaufs nach Müller und Krystek stimmen in vielen Punkten überein. Abb. 9.2 zeigt den Zusammenhang zwischen den Phasen nach Müller und nach Krystek.

Grundsätzlich kann zwischen der schleichenenden und plötzlichen Krise unterschieden werden. Während sich die schleichende Krise langsam über die Zeit hinweg entwickelt, tritt die plötzliche Krise abrupt ein. Jede Krise verläuft in Abhängigkeit von zwei Fakto-

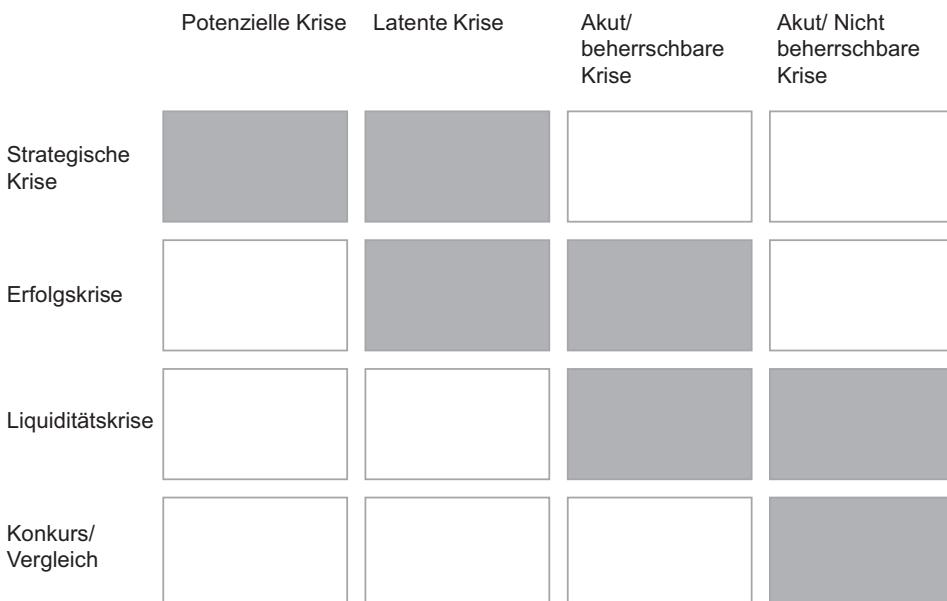


Abb. 9.2 Vergleich der Phasenmodelle nach Krystek und Müller. (Quelle: eigene Darstellung in Anlehnung an Pastors 2002, S. 95)

ren: der Zeit und dem öffentlichen Interesse. Bei der schlechenden Krise steigt das öffentliche Interesse langsam über die Zeit an. Die plötzliche Krise tritt innerhalb kürzester Zeit und im äußersten Fall ohne vorherige Warnung in das öffentliche Interesse. Der Vorteil der schlechenden Krise besteht darin, dass die negativen Auswirkungen nur langsam heranwachsen und damit der zeitliche Handlungsspielraum für die Krisenbewältigung größer ist, als bei der plötzlichen Krise (vgl. Hahn und Ness 2018, S. 44).

Schleichende Krise

Automobilherstellern wird seit Jahren vorgeworfen Abgasmessungen zu manipulieren. Die US-Umweltbehörde geht seit 2015 von einer vorsätzlichen Manipulation aus. Ab diesem Zeitpunkt erhielt der Skandal mehr und mehr öffentliche Aufmerksamkeit. Zunächst klagten vor allem VW-Diesel-Besitzer aus den USA. Volkswagen wurde daraufhin zu Strafzahlungen und Entschädigungen verpflichtet. Es kam vermehrt auch zu Klagen von deutschen VW-Dieselbesitzern (vgl. Ewing 2017, S. 1). Es sind langjährige Prozesse zu erwarten, welche nicht nur das Risiko beinhalten zu Schadenersatz verurteilt zu werden. Diese Prozesse werden von der Öffentlichkeit intensiv verfolgt. Dies erhöht den Druck auf die Politik Verbraucher zu schützen. Der Konzern erleidet auch einen erheblichen Vertrauensverlust. Die Krise brach daher nicht ad-hoc aus, sondern entwickelte sich durch immer mehr Informationen über die Manipulationen und die Klagen über die Zeit.

Plötzliche Krise

Ein Online-Händler besitzt sensible Kundendaten wie Name, Adresse, Kaufverhalten und Kontodaten. Es kommt zu einem Hackerangriff, bei dem die Täter Datenbestände stehlen und die bestehenden IT-Strukturen außer Funktion setzen. Die Internetseite, welche als Online-Shop und als Schnittstelle zwischen den Kunden und dem Unternehmen dient, ist somit für die Kunden nicht mehr zugänglich, um Produkte einzukaufen. Die Folge ist, dass der Online-Händler seine Ware nicht veräußern kann und somit hohe Umsatzeinbußen zu verzeichnen hat. Zusätzlich kommt es zu einem hohen Vertrauensverlust in das Unternehmen aufgrund der gestohlenen Datensätze. Der Vorfall verbreitet sich rasant in den Medien, sodass die Kunden von dem Diebstahl ihrer Daten erfahren und Sorge haben, ob dies negative Folgen für sie haben könnte. Auch potenzielle Kunden haben Bedenken, dem Unternehmen künftig personenbezogene Daten anzuertrauen und verzichten womöglich darauf, Produkte über den Online-Händler einzukaufen.

9.3 Prozess des Schaden- und Krisenmanagements

Im Folgenden wird ein typischer Verlauf eines Schaden- und Krisenmanagements innerhalb eines Unternehmens dargestellt. Dabei wird, trotz der engen Verbundenheit, separat auf das Schadenmanagement und auf das Krisenmanagement eingegangen. Unterteilt ist dies jeweils in die Prävention sowie die Bewältigung von Schäden und Krisen.

9.3.1 Schadenmanagement

Jedem Schadenmanagement gehen innerhalb des Risikomanagements folgende Schritte voraus: Risikoanalyse, Risikovermeidung, Risikoverminderung, Risikotransfer sowie die Festlegung der eigenen Risikotragung. Das Schadenmanagement an sich besteht aus zwei übergeordneten Aufgaben, der Schadenprävention und der Schadenbewältigung. Die Schadenprävention setzt vor Eintritt des Schadens ein, die Schadenbewältigung danach.

In der Schadenprävention sowie in der Schadenbewältigung wird auf jeden einzelnen Schaden eingegangen, wobei der Fokus, im Hinblick auf die Verbundenheit zum Krisenmanagement, auf den Schäden liegt, welche die Existenz des Unternehmens bedrohen bzw. zerstören und somit zu einer Krise führen könnten (vgl. Brauner 2001, S. 10). Kommt es zu einem Schaden, der eine existenzbedrohliche Lage für das Unternehmen verursacht oder dazu in der Lage ist, ist dieser dem Krisenmanagement zuzuordnen. Es liegt im Verantwortungsbereich jedes Unternehmens, selber zu bestimmen, wie es eine Krise definiert sowie festzulegen, wann eine Krise eingetreten ist. Dennoch muss nicht jeder Schaden unmittelbar eine existenzbedrohliche Lage und damit eine Krise nach sich ziehen (vgl. Neubauer 2010, S. 39). Kommt es in einer Produktionsstätte für hochkomplexe elektronische Baugruppen wegen eines technischen Defekts zu einem Feuer, kann aus dem entstandenen (Sach-)Schaden eine Krise für das Unternehmen resultieren. Eine Krise kann bei einem solchen Vorfall leichter ausbrechen, wenn kein angemessenes Schadenmanagement in Verbindung mit dem Risikomanagement implementiert wurde. Als Grundlage für das Schadenmanagement dient das Risikomanagement, welches zum Beispiel für die Festlegung von präventiven Maßnahmen bei Brand sorgt. Beruhend auf diesen Vorgaben, führt das Schadenmanagement die Implementierung von konkreten Brandvermeidungsmaßnahmen durch. Erst durch das Zusammenspiel von Risikomanagement und Schadenmanagement lassen sich Schäden in ihrem Ausmaß verringern oder vermeiden. Beispielsweise fordert das Risikomanagement eine ausreichende Brandbekämpfung, während das Schadenmanagement den Einsatz von Sprinkleranlagen in Produktionsstätten für hochkomplexe elektronische Baugruppen untersagt. Das austretende Wasser von oben, kann zu einem höheren Schaden führen, als ein begrenztes Feuer.

9.3.1.1 Schadenprävention

Die Schadenprävention bezieht sich als Teil des Schadenmanagements auf die Ursache eines Schadens. Sie ist in die zwei Aufgabengebiete, die Schadenvermeidung und die Schadenminderung, unterteilt (vgl. El Hage und Käslin 2006, S. 743). Ziel der Schadenvermeidung ist es, die Schadeneintrittswahrscheinlichkeit zu verringern (vgl. Brauner 2001, S. 5). Die Verhältnismäßigkeit zwischen dem Vermeidungsaufwand und dem Risiko spielt nicht immer eine entscheidende Rolle, weswegen, je nach Schwere des drohenden Schadens oder der drohenden Krise, nicht zwangsläufig eine finanzielle Bewertung der Maßnahmen erfolgen muss. Es sind unter anderem auch Vorbereitungen auf Ereignisse zu treffen, deren Eintrittswahrscheinlichkeit äußerst gering ist, die aber große Auswirkungen haben könnten.

Im Rahmen der Schadenminderung werden Schritte eingeleitet, um zukünftig entstehende Schäden in ihrem Ausmaß verringern zu können, sodass die Entwicklung einer Krise abgewendet werden kann. Die Schadenminderung bereitet auf eine effektive Schadenbewältigung vor (vgl. Brauner 2001, S. 5, 14).

Innerhalb der Schadenprävention gilt es, sich mit möglichen Schadenereignissen vertraut zu machen und Kenntnis über deren Ausmaß und Folgen zu gewinnen. Erst durch diese Vorbereitung kann eine optimale Schadenbewältigung gewährleistet sein. Es ist essenziell, die mögliche Entwicklung des Schadens voraussagen zu können, damit umgehend schadensmindernd agiert werden kann (vgl. Brauner 2001, S. 9). Die Problematik besteht jedoch darin, dass das Unternehmen meist viel zu selten in die Lage gerät, sich mit drastischen Schadenereignissen auseinander setzen zu müssen und daher mit der Situation überfordert ist. Aufgrund dessen ist es wichtig, die Schadenerfahrung nicht nur durch real eingetretene Schäden, sondern auch durch Simulationen und Training zu sammeln. Allerdings wäre es utopisch zu glauben, sich auf jeden erdenklichen Schadenfall im Vorfeld einstellen zu können und für jede wenngleich unwahrscheinliche Situation Vermeidungs- oder Bewältigungsstrategien erarbeiten zu können. Dies würde im Schadenfall ohnehin zu Koordinationsproblemen und somit zu Fehlern führen. Unabhängig davon, was für ein Schaden eingetreten ist, ist das oberste Ziel immer die Existenzsicherung des Unternehmens. Daher ist es im Rahmen der Schadenprävention sinnvoller, die vom Risikomanagement festgelegten Maßnahmen zu implementieren, die nicht nur auf spezifische Schadentypen zugeschnitten sind. Mithilfe der Maßnahmen sollten Krisen möglichst schnell identifiziert und bewältigt werden können (vgl. Brauner 2001, S. 9).

9.3.1.2 Schadenbewältigung

Sobald ein Schaden vorliegt, muss er bewältigt werden. Schäden können in vier verschiedene Stufen eingeteilt werden, welche die Bedeutung der einzelnen Schäden für die Existenz des Unternehmens in Abhängigkeit der zeitlichen Entwicklung darstellen.

Die erste Stufe bildet der Bagatellschaden, welcher die Existenz des Unternehmens nicht gefährdet. Dieser liegt beispielsweise vor, wenn sich ein Mitarbeiter, der als Maschinen- und Anlagenführer für das Unternehmen im Ausland tätig ist, während der Arbeit über ein lose verlegtes Kabel fällt. Bei dem Sturz erleidet er eine Kopfverletzung und ist vorerst für einen Monat krankgeschrieben. Es liegt eine Pflichtverletzung des Arbeitgebers vor, da dieser nicht für die notwendige Arbeitssicherheit gesorgt hat. Diese hat er zu vertreten. Der Personenschaden sowie der damit verbundene Ausfall der Arbeitskraft beeinflussen nicht die Existenz des Unternehmens, welches 200 Mitarbeiter hat. Zudem besteht bezüglich des Falls keine mediale Aufmerksamkeit. Entwickelt sich der Schaden weiter, handelt es sich um einen störenden Schaden. Stellt sich zum Beispiel heraus, dass die Kopfverletzungen Folgeschäden mit sich tragen, sodass eine Invalidität entsteht und der Mitarbeiter nicht mehr seiner Arbeit nachgehen kann, so verbreitet sich dies schnell im Bekanntenkreis des Arbeitnehmers. In dieser Stufe ist die Existenz des Unternehmens noch nicht akut gefährdet. Erst in der dritten Stufe, handelt es sich um eine akute Existenzbedrohung (Krise). Aufgrund des aufgetretenen Falles überprüfen die Behörden die Ar-

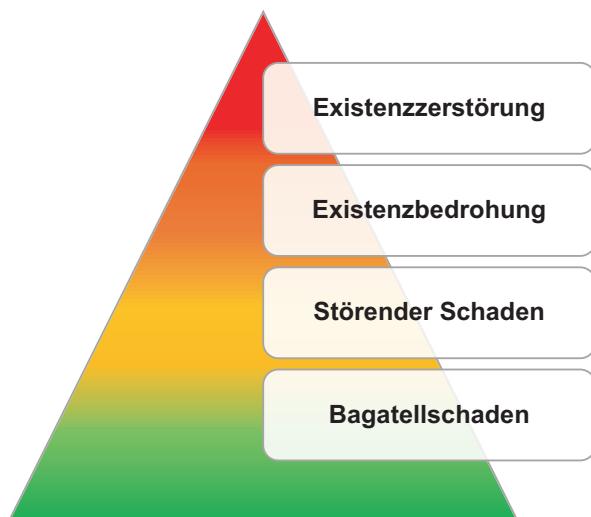
beitssicherheit des Unternehmens und stellen fest, dass diesbezüglich einige Mängel bestehen. Dies zieht die mediale Aufmerksamkeit auf sich. Die Medien haben bereits eine auf das Thema fixierte Öffentlichkeit gefunden. Das öffentliche Interesse steigt immer weiter an, sodass auch ein Großteil der Kunden von der mangelnden Arbeitssicherheit erfährt. Daher kommt es im Unternehmen zu einem starken Rückgang der Verkäufe, was negative wirtschaftliche Folgen nach sich zieht. Entwickelt sich der Schaden weiter, folgt die Existenzzerstörung (Katastrophe) (vgl. Brauner 2001, S. 10). Dies liegt beispielsweise vor, wenn das Unternehmen aufgrund des anhaltenden Rückgangs der Verkäufe in Insolvenz gehen muss. Die Existenzzerstörung muss jedoch nicht zwangsläufig mit der Insolvenz des Unternehmens einhergehen. Bereits der Verlust einer Marktposition stellt eine hohe Gefahr für das Unternehmen dar. Daraus lässt sich erkennen, dass nicht jeder Schaden die Existenz des Unternehmens bedroht und damit eine Krise darstellt (vgl. Neubauer 2010, S. 39). Nur Schäden, welche existenzbedrohend sind, werden dem Krisenmanagement zugeordnet.

Jede Stufe erfordert unterschiedliche Maßnahmen zur Schadensbewältigung. In diesem Zusammenhang ist die Schadenerfahrung von großer Bedeutung (vgl. Abb. 9.3).

9.3.2 Krisenmanagement

Das Krisenmanagement teilt sich in Krisenprävention und Krisenbewältigung. Die Krisenprävention setzt vor Eintritt der Krise ein, die Krisenbewältigung nach der Krise. In der Vergangenheit kam es häufig zu Ereignissen, die erst aufgrund der medialen Aufmerksamkeit zu Krisen geworden sind. Eine fehlende Kommunikation oder Fehler in der Kommunikation können zu einer Verschlechterung der Unternehmenssituation führen (vgl. Pa-

Abb. 9.3 Stufen von Schäden.
(Quelle: eigene Darstellung in Anlehnung an Brauner 2001)



churka und Siegmann 2007, S. 17). Daher nimmt die Einrichtung eines Krisenstabs und die Krisenkommunikation im Rahmen der Krisenprävention- und Bewältigung eine bedeutende Rolle ein.

9.3.2.1 Krisenprävention

Die Ziele der Krisenprävention sind die Krisenvermeidung und Krisenminderung (vgl. Mayer 2003, S. 109). Die Prävention setzt ein, bevor eine Krise entstanden ist. Da nicht alle Krisen vermeidbar sind, ist ein schnelles Handeln bei Kriseneintritt erforderlich. Dies bedarf einer umfassenden Vorbereitung und Planung von Maßnahmen (vgl. Thießen 2014, S. 248).

Zur Krisenprävention zählt die Festlegung eines Krisenstabs. Dieser legt den Grundstein für ein reibungsloses Handeln in der Krisenbewältigung (vgl. Elles 2008, S. 169). Im Falle einer Krise sollte das Unternehmen möglichst schnell entscheiden und handeln. Dazu empfiehlt es sich, für Unternehmen vorab einen Krisenstab aus verantwortlichen Mitarbeitern zu bilden, die sich bei Kriseneintritt unverzüglich an einem vorab festgelegten Ort zusammenfinden (vgl. Nolting und Thießen 2009, S. 156). Dabei bedarf es der Bewertung der aktuellen Krisensituation sowie einer Planung und Dokumentation von Maßnahmen zur Krisenbewältigung in Form eines Krisenplans (vgl. Elles 2008, S. 169). Vor Eintritt der Krise besteht die Aufgabe des Krisenstabs darin, einen Krisenplan vorzubereiten und diesen zu simulieren bzw. zu trainieren. Maßnahmen innerhalb des Krisenplans sind beispielsweise ein Alarm- und Organisationsplan, die Auflistung der Mitglieder des Krisenstabs, Strategien zur Kommunikation sowie die Angabe externer Berater. Hat die Krise bereits eingesetzt, gilt es, den erstellen Krisenplan in die Tat umzusetzen (vgl. Nolting und Thießen 2009, S. 140).

Je nach Unternehmen und eingetretener Krise, kann sich der Krisenstab unterschiedlich zusammengesetzten (vgl. Nolting und Thießen 2009, S. 156). Erfahrungen zufolge wird eine Größe von vier bis zehn Personen für den Krisenstab empfohlen. In Ausnahmefällen kann er auch größer sein. Es sollten sich nur notwendige und damit so wenig Personen wie möglich im Krisenstab befinden. Die Zusammensetzung der Teilnehmer kann sich auch im Verlauf der Krise noch verändern, was jedoch eine Ausnahme darstellen sollte. Die Mitglieder des Krisenstabs werden vorab bestimmt und mit ihren Aufgaben vertraut gemacht. Da sich der Krisenstab vorab gemeinsam auf den Eintritt einer Krise vorbereitet, sind Ihnen die eigenen Aufgaben sowie die Zusammenarbeit als Team bereits geläufig, wenn es tatsächlich zu einer Krisensituation kommt (vgl. Steinke 2018, S. 53). Obwohl die Bestimmung der Krisenstabmitglieder nach unterschiedlichen Kriterien verlaufen kann, sollten folgende Personen einen Sitz im Krisenstab haben: (vgl. Nolting und Thießen 2009, S. 156):

- Mitglied der obersten Führungsebene,
- Kommunikationsverantwortliche,
- Pressesprecher,
- Vertreter der Revision,
- Vertreter der Rechtsabteilung.

Zusätzlich könnten noch folgende Personen erforderlich sein:

- Betriebsratsmitglied,
- Mitglied der Personalleitung,
- Mitglied der Werkleitung,
- Umweltbeauftragte,
- Mitglied der Qualitätssicherung,
- Mitglied aus dem Finanzbereich (bei einer Krise müssen finanzielle Mittel freigesetzt werden).

Dabei sollten alle Krisenstabmitglieder einen Stellvertreter haben (vgl. Pachurka und Siegmann 2007, S. 15). Jeder im Krisenstab erfüllt festgelegte Aufgaben. Wichtige Entscheidungen trifft das Gremium gemeinsam (vgl. Steinke 2018, S. 156). Grundsätzlich ist es wichtig, dass die Aufgabenverteilung klar definiert wurde und jeder sich seiner Rolle innerhalb des Krisenstabs bewusst ist (vgl. Steinke 2018, S. 140). Geht es um wichtige Entscheidungen, so ist der gesamte Krisenstab gefragt. Mindestens ein Krisenstabmitglied sollte, wie oben beschrieben, für die Krisenkommunikation zuständig sein. Das bedeutet, ihm wird die Aufgabe übertragen, den Informationsfluss zu organisieren und zu koordinieren. Dazu sollten bestimmte Abläufe vorbereitet werden. Unter anderem sollte vorab überlegt werden, wie das Unternehmen nach außen und innen aufzutreten hat. Der Auftritt in sozialen Netzwerken, das Intranet sowie die Homepage sollten im Krisenfall rasant ersetzt oder ergänzt werden können. Das bedeutet, dass zum Beispiel die Mitarbeiter der Call Center und Hotlines angeleitet werden sollten, wie der Krisenfall nach außen hin zu kommunizieren ist und welche Informationen gegeben werden dürfen. Es sollte eine sogenannte „Darksite“ vorbereitet werden, die die eigene Homepage während der Krise ergänzen oder ersetzen soll. Dem ganzen Krisenstab sollten die Maßnahmen der Krisenkommunikation geläufig sein. Zusätzlich gibt es noch einen Pressesprecher, dessen Aufgabe es ist, das Unternehmen im Krisenfall zu repräsentieren. Er stellt das „Gesicht“ der Krise für die Öffentlichkeit dar. Um die Aufgabe erfüllen zu können, sollten beispielsweise Trainings vor Mikrofon und Kamera erfolgen. Innerhalb des Unternehmens wird offen kommuniziert, wer im Krisenstab sitzt, damit sich andere Mitarbeiter unter Umständen an diese Personen wenden können (vgl. Nolting und Thießen 2009, S. 156). Es gibt grundsätzlich keine feststehende Regelung oder Empfehlung, aus welchen Personen die Leitung des Krisenstabs bestehen sollte. Die Leitung kann beispielsweise ein Notfall-Manager übernehmen. Der Vorteil ist, dass dadurch die Geschäftsleitung nicht durch diese zusätzliche Aufgabe belastet wird und den Freiraum besitzt, sich um andere Angelegenheiten während der Krise zu kümmern, wie zum Beispiel die Motivation der Mitarbeiter oder die Fortführung des gewöhnlichen Geschäfts (vgl. Steinke 2018, S. 54). In jedem Fall sollten die Ereignisse, bei denen ein Krisenstab einberufen werden soll, klar definiert werden. Ein einheitliches Schema zum Aufbau des Krisenstabs gibt es nicht. Jedes Unternehmen kann frei entscheiden, ob es zum Beispiel nur einen einzigen Krisenstab bildet oder einen zusätzlichen am Einsatzgebiet. Zudem sollte bestimmt werden, wer dazu befugt ist,

den Krisenstab einzuberufen. Auf welche Weise dies geschieht, sollte vorab geklärt werden. Dem Unternehmen ist freigestellt, ob dies zum Beispiel durch SMS oder Anrufe passiert (vgl. Steinke 2018, S. 54). Im Zeitraum zwischen Initiierung eines Alarms und dem Zusammentreffen des Krisenstabs muss die den Alarm auslösende Person die Erstmaßnahmen einleiten und die Leitung übernehmen. Zudem sollte es einen speziellen Raum geben, an denen sich die Mitglieder des Krisenstabs im Krisenfall einfinden (vgl. Steinke 2018, S. 55). Ist die Krise beendet, gibt der Krisenstab Informationen darüber, welche Fehler passiert sind. Daraus können Verbesserungen abgeleitet werden (vgl. Thießen 2014, S. 314).

9.3.2.2 Krisenbewältigung

Die Krisenbewältigung sorgt dafür, dass bereits entstandene Krisen bewältigt werden. Mithilfe von geeigneten Maßnahmen wird versucht, die Krise zu kontrollieren und zu überwinden. Ein wichtiger Bestandteil der Bewältigung ist die Kommunikation.

Die Menschlichkeit steht im Fokus der Krisenkommunikation. Durch das Zeigen von Empathie, Zuverlässigkeit und Lernfähigkeit, lässt sich der (Reputations-)Schaden unter Umständen noch vermindern (vgl. Höbel und Hofmann 2013, S. 21). Reputationsschäden können entstehen, wenn das Krisenmanagement nicht angemessen mit der Krise umgeht und die betriebene Kommunikation ungeeignet war. Dies kann dazu führen, dass interne sowie externe Akteure das Vertrauen in das Unternehmen verlieren (vgl. Thießen 2014, S. 10). Das Hauptaugenmerk der Krisenkommunikation sollte daher auf der Sicherung der Beziehungen zu allen Akteuren liegen. Dies ist essenziell, um die Existenz des Unternehmens zu sichern (vgl. Burmann et al. 2005, S. 464).

Innerhalb der Krisenkommunikation sind vorwiegend drei Schritte zu beachten. Als ersten Schritt sollte das Krisenmanagement allen Akteuren vermitteln, dass sie die Lage sehr ernst nehmen. Dabei sollten Betroffenheit und Mitgefühl glaubwürdig zum Ausdruck kommen. Dazu zählt auch, sich für den (gegebenenfalls) entstandenen Schaden zu entschuldigen. Im zweiten Schritt sollte das Unternehmen vermitteln, dass das Unternehmen die Aufklärung der Krise und damit auch die Aufdeckung der Ursache als höchste Wichtigkeit und Dringlichkeit empfindet. Der dritte Schritt besteht darin, den Schaden zu bewältigen, die Ursache zu beseitigen und damit die Krise zu bekämpfen (vgl. Meckel und Schmid 2008, S. 387).

Grundsätzlich ist bei der Krisenkommunikation die externe und interne Kommunikation zu unterscheiden. Die interne Kommunikation ist auf Mitarbeiter aller Hierarchieebenen ausgerichtet. Unter Umständen werden auch Angehörige in die interne Kommunikation einbezogen. Die externe Kommunikation richtet sich an externe Akteure außerhalb des Unternehmens wie zum Beispiel die Medien, Kunden, Gläubiger, Eigenkapitalgeber und Lieferanten (vgl. Richter 2007, S. 42).

Die interne und externe Kommunikation sollte, je nach Krise unterschiedlich stark ausgeprägt sein. Kommt es beispielsweise zu einer Entführung eines Mitarbeiters während seiner Geschäftsreise im Ausland, liegt der Fokus auf der internen Kommunikation. Die externe Kommunikation sollte möglichst nur begrenzt stattfinden. Handelt es sich um eine

Unterschlagung, sollte die interne Kommunikation auf ein Minimum begrenzt und die externe Kommunikation vermieden werden. Handelt es sich um eine Naturkatastrophe, von der zum Beispiel Mitarbeiter, welche im Ausland für das Unternehmen tätig sind, betroffen sind, sind eine interne sowie eine externe Kommunikation von großer Bedeutung.

Für die Kommunikation mit externen Akteuren, ist das Erstellen einer Kommunikationsstrategie unausweichlich. Da das Ausgesprochene nicht rückgängig gemacht werden kann, sollte sich das Unternehmen vorab über die Botschaft, welche vermittelt werden soll, im Klaren sein. Diese ist den Zuhörern/Zuschauern näher zu bringen (vgl. Höbel und Hofmann 2013, S. 111). Zunächst ist sich bewusst zu machen, wer die Zuhörer/Zuschauer sind. Womöglich haben sie kein oder kaum Fachwissen über das Thema. Es gilt, alles deutlich und für die breite Masse verständlich auszudrücken. Deswegen sollten nur kurze, prägnante Sätze und keine Fachbegriffe, Fremdwörter oder Abkürzungen verwendet werden. Erläuterungen sind mit persönlichen Erfahrungen oder Beispielen zu untermauern. Lügen sind unter keinen Umständen zu verbreiten. Das Unternehmen sollte stets wahrheitsgemäße Aussagen treffen sowie falsche Äußerungen der Presse richtigstellen (vgl. Höbel und Hofmann 2013, S. 111). Es ist besser zuzugeben, etwas (noch) nicht geklärt zu haben, als Spekulationen aufzustellen. Vermutungen sollten keinesfalls mit der Presse geteilt werden. Lediglich Fakten sind an die Öffentlichkeit zu bringen. Der Presse sollte stets mit Lösungsansätzen gegenübergetreten werden. Es empfiehlt sich nicht, erkannte Probleme zu thematisieren (vgl. Meckel und Schmid 2008, S. 386). Außerdem sollten negative Formulierungen vermieden werden. Durch einen positiven, lösungsorientierten und freundlichen Ausdrucksstil wird die ablehnende Haltung der Öffentlichkeit gegenüber dem Unternehmen verbessert (vgl. Höbel und Hofmann 2013, S. 111).

Ist ein Mitarbeiter während seiner Geschäftsreise im Ausland Opfer eines Terroranschlags geworden, spielt die interne sowie externe Kommunikation eine große Bedeutung. In diesem Fall ist die interne der externen Kommunikation zeitlich vorzuziehen. Das bedeutet, dass zunächst die Familie und die Angehörigen des Mitarbeiters zu informieren sind. Im Anschluss erfolgt die erste externe Kommunikation mit außenstehenden Akteuren. Mit den internen Akteuren sollte abgesprochen werden, welche Informationen an die Öffentlichkeit gelangen dürfen. Das Unternehmen steht unter zeitlichem Druck, sich alsbald an die Öffentlichkeit zu wenden, da in vielen Fällen die Medien bereits über den Vorfall berichten. Das Unternehmen sollte sich auf vier Botschaften an die Öffentlichkeit beschränken. Die erste Botschaft beinhaltet das Wissen des Unternehmens über den Vorfall, die zweite eine Information wie weiterhin vorgehen wird. Die dritte Botschaft soll Mitgefühl vermitteln und die vierte die Bekanntgabe, dass weitere Informationen folgen werden. Es gibt einige wichtige Tätigkeiten in der Krisenkommunikation im Falle eines Terroranschlags. Über das Zusammenspiel von Risiko- und Krisenmanagement sollte speziell die Kommunikation mit der Presse durch Zusammenstellung möglicher Fragen und Antworten bzw. vorgefertigter Statements vorbereitet sein. Neue Informationen sind regelmäßig zu veröffentlichen und aktuelle Themen der Öffentlichkeit mit der eigenen Kommunikation abzugleichen.

Nachdem die Krise überwunden wurde, ist das primäre Ziel, des Krisenstabs, die Krise nachzuarbeiten. Der Krisenstab sollte dabei feststellen, welche präventiven sowie bewältigenden Handlungen die Krise positiv und negativ beeinflusst haben. Daher sollte er festhalten, welche Fehler passiert sind und wie diese in Zukunft verhindert werden können. Handlungen, die vom Krisenstab positiv bewertet wurden, sollten beibehalten bzw. nach Möglichkeit optimiert werden.

9.3.3 Praxisbeispiel

Im Folgenden sollen anhand der Risiken für die Mitarbeitersicherheit, wesentliche Aspekte des Prozesses des Schaden- und Krisenmanagements erläutert werden. Dabei sollen vor allem Reiserisiken betrachtet werden, da die Unternehmen ihre Mitarbeiter immer häufiger ins Ausland entsenden. Auch vor dem Hintergrund, dass die mit dem Reisen verbundenen Risiken stetig zunehmen, sollen die Mitarbeiter als größtes Gut des Unternehmens geschützt werden. Je nach Region, sollte sich darauf vorbereitet werden, dass die Mitarbeiter Opfer von Naturkatastrophen (zum Beispiel Erdbeben, Tsunami), Terror (zum Beispiel Bombenanschlag) oder Krankheiten (zum Beispiel Ebolafieber, Coronavirus, Vogelgrippe) werden können. Zum einen ist es für ein Unternehmen ratsam, ein hohes Sicherheitsniveau für den Mitarbeiter zu schaffen, sodass es erst gar nicht dazu kommt, dass der Mitarbeiter zum Beispiel erkrankt oder verletzt wird (vgl. Pachurka und Siegmann 2007, S. 17). Dies geschieht im Rahmen des Schadenmanagements. Zum anderen sollte sich auf den Krisenfall vorbereitet werden (vgl. Pachurka und Siegmann 2007, S. 17). Dies erfolgt im Rahmen des Krisenmanagements.

Das Schadenmanagement und insbesondere die Schadenprävention sieht eine Umsetzung der vom Risikomanagement vorgegebenen Reiserichtlinien zur Vermeidung von Personenschäden vor. Dabei ist es empfehlenswert eine Gefährdungsbeurteilung und Checklisten zu verwenden. Die Gefährdungsbeurteilung dient der Vermeidung von Schäden (und einer Weiterentwicklung zur Krise), indem ermittelte Gefährdungen weitestgehend minimiert oder sogar eliminiert werden. Unter die Gefährdungsbeurteilung zählt zusätzlich die Minderung von Schäden, indem Schutzmaßnahmen getroffen werden. Bevor Mitarbeiter ins Ausland geschickt werden, ist im Rahmen des Schadenmanagements eine umfassende Gefährdungsbeurteilung, welche aus sieben Schritten besteht, durchzuführen (vgl. zum gesamten Beispiel Balme et al. 2018, S. 11 ff.):

1. Arbeitsbereiche und Tätigkeiten festlegen
2. Gefährdungen ermitteln
3. Gefährdungen beurteilen
4. Maßnahmen festlegen
5. Maßnahmen durchführen
6. Maßnahmen auf Wirksamkeit überprüfen
7. Gefährdungsbeurteilung fortschreiben

Der erste Schritt umfasst eine Evaluierung von Gesetzen und Vorschriften sowie eine Festlegung von Tätigkeiten und Verantwortlichkeiten.

Als rechtliche Grundlage dient unter anderem das Arbeitsschutzgesetz. § 5 ArbSchG besagt, dass der Arbeitgeber die Pflicht hat, Gefährdungen zu beurteilen. Verantwortlichkeiten werden festgelegt, indem beispielsweise Fachkräfte für Arbeitssicherheit und Betriebsärzte den Unternehmer zum Arbeitssicherheitsgesetz beraten. Zudem sollte der Arbeitgeber sowie die Mitarbeiter die Möglichkeit haben, sich von einem Reisesicherheitsexperten zu Sicherheitsrisiken des jeweiligen Landes beraten zu lassen.

Der zweite Schritt dient der Ermittlung von Gefährdungen. Die Gefährdungen betreffen das Reiseland, den Reisenden, das Unternehmen und die Reisepläne. Die Erstellung eines Profils des Reisenden dient der Ermittlung der psychischen und physischen Gesundheit. Dazu gehören die Berücksichtigung von Geschlecht, Grunderkrankungen, Alter, Reiseerfahrung und berufliche oder gesellschaftliche Stellung des reisenden Mitarbeiters. Dadurch können Personengruppen identifiziert werden, die besonders gefährdet sind. Gemeint sein können unter anderem Personen, die eine gewisse Krankenvorgeschichte haben und deren Krankheit sich in dem jeweiligen Land verschlimmern bzw. erneut ausbrechen könnte. Auch Mitarbeiter, welche eine besonders hohe Stellung im Unternehmen innehaben, könnten von einem höheren Risiko, entführt zu werden, betroffen sein. Je nachdem um welches Unternehmen es sich handelt, sind unterschiedliche Gefährdungen zu beachten. Beispielsweise sind kaufmännische Angestellte anderen Gefahren ausgesetzt, als Bauarbeiter oder Journalisten.

Nicht nur das Land an sich, sondern auch der genaue Ort, an den der Mitarbeiter geschickt wird, muss auf seine Gefahren hin analysiert werden. Dabei müssen verschiedene Gegebenheiten Berücksichtigung finden, wie zum Beispiel die geografische Lage, die Kriminalitätsrate, der Entwicklungsstand sowie die Infrastruktur. Zusätzlich sind medizinische Risiken des Reiselandes zu berücksichtigen wie zum Beispiel Infektionskrankheiten, medizinische Infrastruktur, spezielle Gefahren vor Ort (Hygiene, Klima usw.) und psychische Belastungen. Die Länder können je nachdem wie risikoreich sie sind, in Risikoklassen eingeteilt werden. Hierfür bietet sich eine Risikoklassifizierung der Länder zum Beispiel anhand der Dokumentationen des Auswärtigen Amtes an. Je höher die Risikoklasse, desto höher sind die Anforderungen an das Schaden- und Krisenmanagement. Zudem ist der zeitliche Reiseplan bei der Ermittlung des Risikos von Bedeutung, da bestimmte Ereignisse die Gefahrenlage verändern können. Dazu zählen zum Beispiel religiöse oder politische Ereignisse wie Wahlen oder Feiertage.

Der dritte Schritt besteht aus der Beurteilung der Gefährdung. Diese erfolgt für jeden Arbeitsplatz bzw. jeden Arbeitsprozess. Analysiert wird der Zielort auf Bedrohungen und örtliche Gefahren. Unter Bedrohungen werden Kriminalität, Terrorismus, soziale Unruhen und Konflikte verstanden. Örtliche Gefahren gehen aus von dem Straßenverkehr, inländischen Reisen, kulturellen Aspekten sowie Naturkatastrophen.

Obwohl eine solche Gefährdungsbeurteilung nicht für die Angehörigen des im Ausland befindlichen Mitarbeiters erstellt wird, ist es für den Arbeitgeber empfehlenswert, die An-

gehörigen des Mitarbeiters zur Beruhigung auf die Existenz des Reisemanagements hinzuweisen.

Die, aus den Gefährdungen abgeleiteten Maßnahmen, werden im Rahmen des vierten, fünften und sechsten Schritts festgelegt, durchgeführt und anschließend auf ihre Wirksamkeit überprüft.

Bei Zielorten mit besonders hohem Gefährdungspotenzial kann für Reisende ein Personenschutz als zusätzliche Schutzmaßnahme notwendig sein. Sinnvoll ist es, vorab festzulegen, bei welchen Risiken ein solcher erforderlich ist.

Zu beachten ist auch, welche Unterkünfte dem Mitarbeiter zur Verfügung gestellt werden. Wie hoch der Sicherheitsstandard der Unterkunft sein muss, ist abhängig von den bereits ermittelten Gefährdungen. Dabei erfolgen zum Beispiel Bewertungen hinsichtlich getroffener Brandschutzmaßnahmen, Zugangskontrollen und das Vorhandensein von Sicherheitspersonal.

Da jede Reise mit unterschiedlichen Risiken verbunden ist, sollte die Maßnahmenliste mithilfe der siebten Phase immer wieder erweitert, aktualisiert und dokumentiert werden.

Mithilfe von vorab angefertigten Checklisten kann der Arbeitgeber evaluieren, ob er die erforderlichen Maßnahmen eingehalten hat.

Im Rahmen des Krisenmanagements sind für die Krisensituation folgende organisatorische Vorbereitungen zu treffen:

1. Dem Mitarbeiter ist eine App oder Notrufnummer zur Verfügung zu stellen, die es ihm möglich macht mit der Notrufzentrale zu kommunizieren und bei Bedarf einen Notruf abzusetzen. Es sollte möglich sein, den Ort des Notrufes des Mitarbeiters mithilfe eines Trackingverfahrens zu lokalisieren.
2. Die Notrufzentrale muss ständig besetzt sein. Mehrsprachigkeit ist hier sicherzustellen.
3. Die Notrufzentrale muss nach der Art der Krise Telefonnummern von verantwortlichen Personen des Krisenstabes vorliegen haben, damit anlassbezogen reagiert werden kann. Eine vollständige und aktuelle Telefonliste ist von entscheidender Bedeutung, damit die Erreichbarkeit des Krisenstabes sichergestellt ist.
4. Es muss sichergestellt sein, dass die erreichte Person die anderen Mitglieder des Krisenstabes erreichen und den Krisenfall somit auslösen kann.
5. Ein Krisenraum ist vor Eintritt der Krise festzulegen und jedem Krisenmitglied bekannt zu geben. Im Krisenfall haben sich sämtliche Mitglieder des Krisenstabes dort zu versammeln.
6. Vor Kriseneintritt werden die Rollen, welche jedes Krisenstabsmitglied übernehmen soll, festgelegt. Zum Beispiel wird festgehalten wer die Rolle Protokollführers oder des Kommunikationsverantwortlichen mit der Behörde oder den Medien übernimmt. Im Krisenfall hat sich jeder seiner Rolle innerhalb des Stabs bewusst zu sein. Jedes Krisenstabsmitglied sollte mit seinen eigenen Aufgaben vertraut sein. Dazu dienen E-Learning, Simulationen und Rollenspiele.

9.4 Schluss und Ausblick

Besondere und außergewöhnliche Umstände können Unternehmen erheblich belasten und gegebenenfalls auch existenzbedrohend sein. Durch ein systematisches Schaden- und Krisenmanagement kann und muss sich ein Unternehmen darauf vorbereiten. Dies ist die unternehmerische Pflicht eines jeden Unternehmens. Klare Strukturen gepaart mit Zuständigkeiten, Verantwortlichkeiten und Erreichbarkeit des Krisenstabs sind zwingend erforderlich, um Krisen angemessen zu begegnen. Aber nur personelle Ressourcen vorzuhalten reicht nicht aus. Es müssen auch technische Voraussetzungen für die Kommunikation (zum Beispiel ausgestatteter Krisenraum) vorgehalten werden. Der Umgang mit Krisen sollte auch trainiert werden, damit im Krisenfall zielgerichtet und schnell reagiert werden kann. Das Schaden- und Krisenmanagement ist regelmäßig auf Anpassungsnotwendigkeiten hin zu überprüfen, da interne und externe Risiken einem Änderungsprozess unterliegen.

Literatur

- Balme, F. et al. (2018). Leitfaden zur Erstellung der Gefährdungsbeurteilung. <https://www.sicherheit-das-fachmagazin.de/app/download/11643812/Leitfaden+Gef%C3%A4hrdungsbeurteilung.pdf>. Zugegriffen am 21.02.2020.
- Brauner, C. (2001). *Präventive Schadensbewältigung: Mehr gewinnen als verlieren*. Zürich: Swiss Re Publishing.
- Brühl, K. et al. (2018). Sicherheits- und Krisenmanagement als Kern eines integrativen Risikomanagements. *Risiko Manager*, 4, 4–8.
- Burmann, C., Freiling, J., & Hülsmann, M. (2005). *Management von Ad-hoc-Krisen: Grundlagen – Strategien – Erfolgsfaktoren* (1. Aufl.). Wiesbaden: Gabler.
- El Hage, B., & Käslin, B. (2006). Funktionen der Versicherung in der Schadenprävention. *Zeitschrift für Versicherungswesen*, 22, 743–747.
- Elles, A. (2008). *Risiken vermeiden – Krisen bewältigen* (1. Aufl.). Hamburg: B. Behr's.
- Evertz, D., & Krystek, U. (2014). *Unternehmen erfolgreich restrukturieren und sanieren: Herausforderungen und Lösungsansätze für den Turnaround* (1. Aufl.). Stuttgart: Schäffer-Poeschel.
- Ewing, J. (2017). *Wachstum über alles: Der VW-Skandal: Die Personen. Die Technik. Die Hintergründe* (1. Aufl.). München: Droemer HC.
- General Manager Central Europe der International SOS. (2012). Entsendung von Mitarbeitern in potenzielle Krisengebiete. *Die VersicherungsPraxis*, 2, 21–23.
- Hahn, S., & Ness, Z. (2018). *Krisenkommunikation in Tourismusorganisationen: Grundlagen, Praxis und Perspektiven*. Wiesbaden: Springer Fachmedien.
- Höbel, P., & Hofmann, T. (2013). *Krisenkommunikation* (2. Aufl.). Konstanz/München: UVK Verlagsgesellschaft.
- Hustedt, T. (2019). Verwaltung und der Umgang mit Krisen und Katastrophen. In S. Veit, C. Reichard, & G. Wewer (Hrsg.), *Handbuch zur Verwaltungsreform* (S. 2–10). Wiesbaden: Springer VS.
- Krystek, U. (1987). *Unternehmungskrisen: Beschreibung, Vermeidung und Bewältigung überlebenskritischer Prozesse in Unternehmungen* (1. Aufl.). Wiesbaden: Gabler.
- Martin, T., & Bär, T. (2002). *Grundzüge des Risikomanagements nach KonTraG: Das Risikomanagementsystem zur Krisenfrüherkennung nach § 91 Abs.2 AktG*. München: Oldenbourg.

- Mayer, V. (2003). *Operatives Krisenmanagement: Grundlagen, Methoden und Werkzeuge des ganzheitlichen Risk Management* (1. Aufl.). Wiesbaden: Deutscher Universitätsverlag GmbH.
- Meckel, M., & Schmid, B. (2008). *Unternehmenskommunikation: Kommunikationsmanagement aus Sicht der Unternehmensführung* (2. Aufl.). Wiesbaden: Gabler GWV Fachverlage.
- Neubauer, M. (2010). *Krisenmanagement in Projekten: Handeln, wenn Probleme eskalieren* (3. Aufl.). Heidelberg: Springer.
- Nolting, T., & Thießen, A. (2009). *Krisenmanagement in der Mediengesellschaft, Potenziale und Perspektiven der Krisenkommunikation* (1. Aufl.). Wiesbaden: VS.
- Pachurka, C., & Siegmann, S. (2007). Krisen erkennen, bewältigen und vorbeugen – Unternehmenswerte proaktiv schützen. *Praktische Arbeitsmedizin*, 8, 12–17.
- Pastors, P. M. (2002). *Risiken des Unternehmens: Vorbeugen und meistern*. München/Mering: Rainer Hampp.
- Richter, N. (2007). *Interne Kommunikation im Krisenmanagement* (1. Aufl.). Siegburg: Josef Eul.
- Rohlf, T. (2018). *Risikomanagement im Versicherungsunternehmen: Identifizierung, Bewertung und Steuerung*. Karlsruhe: Versicherungswirtschaft.
- Sieg, I. (1999). *Krisenmanagement im Versicherungsunternehmen*. Karlsruhe: Versicherungswirtschaft GmbH.
- Steinke, L. (2018). *Kommunizieren in der Krise: Nachhaltige PR-Werkzeuge für schwierige Zeiten* (2. Aufl.). Wiesbaden: Springer Gabler.
- Thierhoff, M., & Müller, R. (2016). *Unternehmenssanierung* (2. Aufl.). Heidelberg: C.F. Müller.
- Thießen, A. (2014). *Handbuch Krisenmanagement* (2. Aufl.). Wiesbaden: Springer VS.

Michael Seidl hat nach einer Ausbildung zum Industriekaufmann ein Studium der Rechtswissenschaften und der LMU-München absolviert und war in der Folge in diversen Fach- und Führungspositionen bei den drei weltweit agierenden Industrieversicherungsmaklern Aon, Willis und Marsh tätig. Seit 2012 ist er beim firmenverbundenen Versicherungsvermittler des internationalen Automobilzulieferers Dräxlmaier als Prokurist mit Schwerpunkt Haftpflicht und Transport tätig. Daneben ist er Teil des Teams der Rechtsabteilung des Konzerns, wo er die Bereiche Zoll und Außenwirtschaft, Frachtrecht und Produkthaftung verantwortet und ist Mitglied des Teams Risikomanagement des Konzerns.

Kathrin Regeling studierte Versicherungswesen mit den Schwerpunkten Sach- und Betriebsunterbrechungsversicherung, Haftpflicht-/ Unfall-/ Kraftfahrt-/ Rechtsschutzversicherung und Rechnungswesen von Versicherungsunternehmen am Institut für Versicherungswesen der Technischen Hochschule Köln. Im Anschluss absolvierte sie dort auch das Masterstudium Risk & Insurance.



Business Continuity Management

10

Vorbereitung auf den Notfall

Marco Mirkes und Emine Özcan

Zusammenfassung

Ein funktionierendes Business Continuity Management (BCM) hilft existenzielle Krisen in Unternehmen zu bewältigen. Schadenprävention und Transfer der klassischen Risiken wie Feuer, Explosion oder Naturgefahren an Versicherungen sind schon länger nicht mehr als alleinige Absicherung gegen Unternehmensrisiken ausreichend. Szenarien für politische Risiken, Hackerangriffe, Datendiebstahl sowie Ausfall von IT-Systemen, kritischer Infrastruktur oder von Know-How-Trägern im Unternehmen stellen weitere Gefahren dar, die durch das BCM im Detail analysiert und bewertet werden sollten. Mithilfe der Auswirkungsanalyse auf erkannte Bedrohungen können zur Prävention gezielt Gegenmaßnahmen definiert werden. Das Ziel eines BCM ist es, die Fortführung der Geschäftstätigkeit nach einem Schadeneignis zu sichern und dadurch Kosten zu reduzieren. Durch das BCM soll ein Prozess erstellt werden, der unter Optimierung von Ressourcen und Mitteln im Unternehmen einen adäquaten Schutz für benannte Gefährdungen aufbaut. Durch die Vorbereitung auf die Bedrohungen können die Auswirkungen reduziert oder auf ein akzeptiertes Maß begrenzt und somit für das Unternehmen kontrollierbar und planbar gemacht werden.

M. Mirkes (✉)

Generali Versicherung AG, München, Deutschland

E-Mail: marco.mirkes@general.com

E. Özcan

TH Köln, Institut für Versicherungswesen, Köln, Deutschland

E-Mail: emine.oezcan96@gmail.com

10.1 Business Continuity Management

10.1.1 Was ist BCM?

Business Continuity Management (BCM) ist ein ganzheitlicher Prozess, der Unternehmen dabei unterstützt potenzielle Bedrohungen und deren Einfluss auf ihre Geschäftsprozesse zu identifizieren. Neben den klassischen Störfallereignissen wie Maschinenbruch, Feuer oder Naturgefahren werden neue Szenarien wie Bedrohung durch Hacker, Ausfall der IT oder Verschiebungen des Marktgleichgewichts immer wichtiger für Unternehmen und die Bewältigung derartiger Bedrohungen, die in der Folge bis hin zur Insolvenz reichen können, immer bedeutender. Gesetzgeber und Aufsichtsbehörden erkennen diesen Trend und geben zum Beispiel im Finanzsektor mit neuen Ansätzen zum operationellen Risikomanagement Regeln vor.

Business Continuity Management wird auch als Betriebskontinuitätsmanagement (BKM) oder Geschäftsfortbestandsmanagement (BFM) bezeichnet. Es hat sich zu einem Ansatz des Krisen- und Risikomanagements entwickelt und wird meist organisationsweit angewandt. Das BCM beinhaltet Pläne, Strategien und Handlungen, um Prozesse zu schützen und im Notfall alternative Abläufe ohne Verzögerung zu ermöglichen. Es umfasst somit die Elemente Erkennen von Bedrohungen, Analyse von Risiken, Planung und Vorbereitung auf die Krise, das Krisen- und Notfallmanagement, Test- und Übungsprozeduren und die Dokumentation des Plans. In erster Linie betrifft ein BCM die wertschöpfenden Prozesse, also das Kerngeschäft (vgl. Von Rössing 2005, S. 34). Hierbei werden Bereiche, bei denen der Verlust für das Unternehmen am größten ist, in den Vordergrund gestellt.

BCM stellt Unternehmen ein Rahmenwerk für die Optimierung der eigenen Widerstandsfähigkeit gegen Bedrohungen bereit und bietet die Möglichkeit, die Interessen der Stakeholder, die Reputation des Unternehmens, die Marke und die Wertschöpfung zu sichern. Durch das BCM wird versucht eine Krise kontrolliert zu überwinden und dabei die Auswirkungen zu begrenzen

Nach Identifikation aktueller und möglicher Bedrohungen des Unternehmens wird eine detaillierte Analyse der Risiken durchgeführt. Für die Bedrohungen mit den größten Risiken werden Maßnahmen oder Vorbereitungen getroffen, um bei einem Ereignis die Situation im Unternehmen im Ausmaß zu begrenzen und das Ereignis zu kontrollieren.

Ein funktionierendes BCM muss gut in die bestehende Struktur des Unternehmens integriert sein und Schnittstellen zum Management haben. Durch die systematische Be trachtung und Bewertung ganz unterschiedlicher Unternehmensrisiken aus den verschiedenen Geschäftsbereichen und Unternehmenssegmenten schafft das BCM eine bessere Übersicht über die tatsächliche Risikolandschaft.

10.1.2 Ziele des BCM

Statistisch tritt alle drei Jahre ein geschäftsgefährdendes Ereignis in einem Unternehmen ein. Diese Ereignisse haben bei ungünstigem Verlauf auch das Potenzial massive Schäden an Unternehmenswerten oder Ressourcen zu verursachen. Es gibt Untersuchungen, die besagen, dass 90 Prozent der Unternehmen, welche auf solch ein Ereignis nicht mit geeigneten Gegenmaßnahmen reagieren konnten, innerhalb von 24 Monaten vom Markt verschwunden sind (vgl. Müller 2014, S. 339 ff.).

Unternehmerische Tätigkeit ist stets mit Unsicherheiten verbunden. Auf der anderen Seite sind Unternehmen aber auch bestrebt möglichst viele der vorhandenen Unsicherheiten zu kontrollieren oder zu beseitigen.

Die Kernaufgabe des BCM besteht darin, den Fortbestand des Unternehmens unter primärer Beachtung von Risiken mit hohem Schadensausmaß zu sichern (vgl. Spörer 2014, S. 48). Dies gelingt dadurch, dass Ausfälle kritischer Abläufe und Ressourcen proaktiv untersucht werden und realistische Strategien und konkrete Pläne für die Reduzierung der negativen Auswirkungen entwickelt werden (vgl. GDV, S. 5). Für erkannte kritische Ressourcen in einem Unternehmen werden im BCM Notfallpläne (sogenannte Business-Continuity-Pläne) erarbeitet, getestet und regelmäßig überprüft. Hierdurch wird bei Ausfall kritischer Ressourcen ein geordneter Notbetrieb und im Anschluss eine strukturierte Wiederherstellung des Normalbetriebs sichergestellt (vgl. GDV 2018, S. 7).

Die größten Vorteile des BCM liegen in der aktiven Minimierung von Auswirkungen von Ereignissen und der Minimierung der Ausfallzeit nach einer Störung. Außerdem gewährleistet das BCM die kontrollierte Abarbeitung der wichtigsten Aufgaben im Unternehmen während einer Krise, ohne sich von Ereignissen treiben zu lassen. Durch das BCM ist das Unternehmen auf eine Krise vorbereitet, indem es eine geplante Vorgehensweise für unterschiedliche Szenarien fixiert und getestet hat.

10.1.3 Elemente des BCM-Lebenszyklus

Im Laufe der Zeit wurden verschiedene Modelle zur Durchführung und Systematisierung des BCM entwickelt. In der Praxis haben sich sieben Kernelemente sowohl für die geschäftliche als auch für die technische Perspektive durchgesetzt. Neben den operativen Phasen Verständnis der Organisation, Implementierung, Testen, Prüfen und Auswerten sind dabei Projektmanagement und Einbettung des BCM in die Unternehmenskultur definierte Querschnittsaufgaben. Der Lebenszyklus sichert die Entwicklung und Nachhaltigkeit eines Business Continuity Managements.

Abb. 10.1 zeigt die verschiedenen Phasen, die zentral vom Programmmanagement gesteuert werden. Die einzelnen Phasen des BCM-Lebenszyklus sollen nicht als Einzelprojekte betrachtet werden, sondern als ein Gesamtprojekt mit aufeinander aufbauenden Projektphasen. Das BCM-Konzept orientiert sich an einem Reifegradmodell, das die

Abb. 10.1 BCM-Lebenszyklus. (Quelle: eigene Darstellung in Anlehnung an BCI 2010, S. 20)



Verbesserung über mehrere Jahre messbar macht. Prüfung und Revision der BCM-Fähigkeit sind integraler Bestandteil des Gesamtmodells (vgl. von Rössing 2005, S. 70 f.).

Die einzelnen Phasen des BCM-Lebenszyklus beinhalten ein definiertes Arbeitsprogramm, das der Zielvorgabe als auch der Fortschrittskontrolle und der Prüffähigkeit dient. Dieser muss individuell an das Unternehmen angepasst werden, da jedes Unternehmen sich hinsichtlich Organisation, Geschäftsprozessen und Grad der Digitalisierung unterscheidet. Es gibt keinerlei Vorschriften über die Verteilung der Zuständigkeiten und Kompetenzen (außer der Revision). Daher besteht die Möglichkeit ein Teil des Projektes oder das gesamte Projekt an externe Berater zu übertragen.

10.1.4 Rechtlicher Rahmen

Im Gegensatz zu anderen Fachdisziplinen zeigt sich im betrieblichen Kontinuitätsmanagement eine übersichtliche Vorschriftenlage, was zum einen zwar wenig Führung für die Erstellung vorgibt, zum anderen aber umso mehr Freiheiten für die Umsetzung ermöglicht. Es existiert kein einheitliches BCM-Gesetz, das Prinzipien und Maßnahmen abschließend regelt. Vielmehr sind Hinweise in einzelnen Fachbereichen vorhanden, wie und in welchem Umfang ein BCM-System gestaltet werden soll. Im Folgenden ein kurzer Einblick in die allgemeinen sowie rechtlichen Grundlagen.

ISO-Norm 22301

Die Norm ISO 22301 enthält eine Reihe von Anforderungen zur Erstellung und zum Umgang mit dem Business Continuity Management-System und stellt somit den Rahmen für das Business Continuity Management eines Unternehmens. Sie gilt als universell in dem Sinne, dass sie auf Unternehmen jeglicher Größe anwendbar und unabhängig von den eingesetzten Technologien ist (vgl. International Organization for Standardization 2012).

Der Standard spezifiziert die Anforderungen für Planung, Implementierung, Durchführung, Kontrolle, Bewertung und kontinuierliche Verbesserung eines dokumentierten BCM-Systems.

Standard BSI-100-4

Dieser Standard kommt aus dem Bereich IT-Sicherheit und beschreibt wie die klassische IT-Grundschutz-Vorgehensweise gemäß BSI-100-2 zusammen mit der Risikoanalyse gemäß BSI-100-3 als Basis für eine angemessene Vorsorge zur Vermeidung von Notfällen verwendet werden kann (vgl. BSI 2008).

Im BSI-Standard wird eine Methodik zur Etablierung und Aufrechterhaltung eines behördlichen- bzw. unternehmensweit internen Notfallmanagements vorgestellt. Ziel des Standards ist es, einen systematischen Weg aufzuzeigen. Dadurch soll bei Notfällen und Krisen, die zu einer Geschäftsunterbrechung führen können, eine schnelle Reaktion ermöglicht werden.

10.1.5 Schnittstellen und Grenzen des BCM

Durch das betriebliche Notfallmanagement werden organisatorische, personelle und sachliche Voraussetzungen innerhalb der normalen Betriebsorganisation geschaffen, um auf Notfälle angemessen reagieren zu können. Das Notfallmanagement hat die Aufgabe der Abwehr oder der Begrenzung primärer Gefahren, zum Beispiel gezieltes Abschalten von Anlagen oder durch Aktivieren der Betriebsfeuerwehr. Reichen die durch das Notfallmanagement eingeleiteten ersten Maßnahmen zur Bewältigung von Notfällen nicht aus oder droht eine weitere Eskalation, wird aus dem Notfallmanagement heraus das Krisenmanagement aktiviert. Da im Notfallmanagement und Krisenmanagement teils ganz unterschiedliche Verantwortlichkeiten, Schutzziele und Strategien bestehen, ist es notwendig eine Schwelle zu definieren ab wann eine Krise ausgelöst wird und das Krisenmanagement startet. Der Aufbau eines funktionierenden Krisenmanagements ist Teil des BCM.

Das Krisenmanagement im weiten Sinne setzt sich mit allen Phasen einer Krise, von einer potenziellen bis hin zu einer akuten, nicht beherrschbaren Krise auseinander (vgl. Bergauer 2003, S. 6). Die Zielsetzung des Krisenmanagements ist das Führen und somit das Planen, Steuern und Kontrollieren zur Vermeidung oder Bewältigung überlebenskritischer Prozesse in Unternehmen. Krisenmanagement muss in engem Zusammenhang mit dem Risikomanagement gesehen werden. Der Unterschied zwischen Risikomanagement und Krisenmanagement besteht in erster Linie darin, dass Risikomanagement versucht

möglichst quantitative Aussagen über bekannte und zu erwartende Risiken zu treffen und beim Krisenmanagement darin möglichst genaue Szenarien vorzubereiten, mit denen bei Eintritt eines Risikos reagiert werden kann (vgl. Krystek 1987, S. 27 f.).

Notfallmanagement und Krisenmanagement/Business Continuity Management sind Bestandteile des übergeordneten Risikomanagements.

„Das Business Continuity Management lebt im Unternehmen nur so gut, wie es kulturell akzeptiert wird.“, stellt von Rössing in seinem Buch „Betriebliches Kontinuitätsmanagement“ fest. Nur eine plausible Vermittlung der Werte des BCM durch das Management bringt ausreichende Akzeptanz und Unterstützung für die teils aufwändigen und technisch geprägten Aufgaben und Analysen, zumal Ressourcen und Zeit für die Durchführung in der Regel für die Ausführenden knapp bemessen und begrenzt sind. Der Pflege der BCM-Kultur kommt im Rahmen des BCM-Lebenszyklus eine wichtige und fortwährende Aufgabe zu, die sich schwer in Phasen einteilen lässt. Es ist jedoch entscheidend, dass die Notwendigkeit für die Durchführung und die Bedeutung des BCM für das Unternehmen in allen Ebenen des Unternehmens verstanden und akzeptiert wird.

Krisen, Notsituationen und unvorhergesehene Ereignisse sind ebenso wie Ordnung, Kontinuität und Sicherheit entscheidende Einflussfaktoren für einen Menschen. Die Einstellung des Einzelnen zu diesen Punkten prägt sein Verhalten und beeinflusst damit auch die Handlungen im Unternehmen.

Höchste Priorität beim Aufbau eines BCM besitzt die sogenannte BCM-Richtlinie (BCM-Policy). Diese definiert den Anwendungsbereich des BCM in einer Organisation und legt die wesentlichen Grundlagen für den späteren Erfolg. In der BCM-Richtlinie wird von der Unternehmensleitung auch festgelegt, dass BCM ein integraler Bestandteil der Unternehmenspolitik ist. Des Weiteren gibt die Unternehmensleitung vor, wie und in welcher Höhe notwendige Ressourcen zum Aufbau und Betrieb eines BCM bereitgestellt werden. Die BCM-Richtlinie ermöglicht somit ein effizientes und effektives BCM, sichergestellt durch einen klar definierten Geltungsbereich (vgl. GDV 2018, S. 6 f.).

10.2 Umsetzung eines Business Continuity Managements

10.2.1 Projekt- und Programmmanagement

Aufgrund der vielen betroffenen Unternehmensbereiche und auszuführenden Tätigkeiten erfordert das Business Continuity Management ein definiertes Projekt- und Programmmanagement. Das Management des BCM-Programms und der darunter gruppierten Projekte ist hierbei eine zentrale Funktion innerhalb des BCM-Lebenszyklus, da hierüber die BCM-Prozesse, der Qualitätssicherungsprozess und das Krisenmanagement im Unternehmen definiert werden. Im Vordergrund stehen also nicht Inhalte, sondern die Umsetzung des BCM. Erforderlich für die inhaltliche Gestaltung des Business Continuity Management sind begleitende Rahmenrichtlinien und die fortlaufende Unterstützung auf allen

Managementebenen. Ebenfalls sind Überwachung und Kontrolle der Projekte mithilfe standardisierter Verfahren des Projektmanagements von Bedeutung. Als Konsequenz aus den übergeordneten Anforderungen ergeben sich folgende Ziele:

- Sicherstellung einer effektiven und anhaltenden BCM-Fähigkeit des Gesamtunternehmens
- Effizientes und dem Zweck angemessenes Management des BCM-Programms
- Bereitstellung eines integrierten Managementprozesses mit BCM als festem Bestandteil des allgemeinen Managements
- Festlegung der Rechenschaftspflicht für das BCM gegenüber den Fachbereichen und den dort Verantwortlichen (vgl. von Rössing 2005, S. 387 f.)

Im Zuge des Projektmanagements werden diese Ziele als Meilensteine bei der Umsetzung aufgefasst. Gegenstand des Projektmanagements ist zudem die Überwachung der zeit- und budgetgerechten Erreichung der Ziele. Zudem sind Komponenten wie BCM-Politik, definierte Grundprinzipien des BCM, BCM-Standards, BCM-Handlungsrahmen, Finanzierungskonzept, Ressourcenzuweisung, Revisionsplanung sowie Qualitätssicherung für das BCM Mindestanforderungen im Rahmen des BCM-Programms.

Die Meilensteine des Projektstrukturplans ergeben sich aus dem Abschluss der Phasen im BCM-Lebenszyklus. Abb. 10.2 zeigt eine vereinfachte Darstellung des Lebenszyklus für das BCM-Programm.

Die grundlegenden Kenngrößen (Sachziel, Zeitplan und Ressourcenplan) sind, wie in jedem anderen Projekt, zu überwachen.

Das Projekt zur Erstellung der ersten Version eines BCM-Programms sollte eine in sich abgeschlossene, abnahmefähige Einheit darstellen. Das Sollergebnis wird vor der Übernahme des BCM in einen regulären, fortlaufenden Geschäftsprozess überprüft (vgl. von Rössing 2005, S. 397 f.).

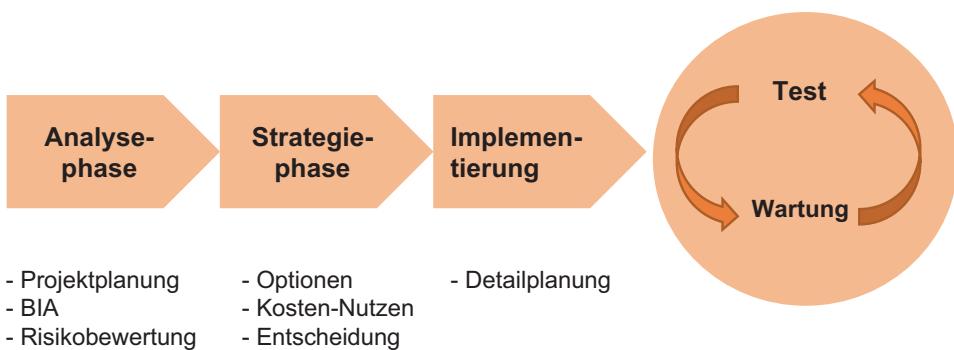


Abb. 10.2 Lebenszyklus für BCM-Programm. (Quelle: eigene Darstellung in Anlehnung an von Rössing 2005, S. 391)

10.2.2 Planen – Organisation verstehen

Das Verständnis der eigenen Geschäfts- und Unternehmensabläufe ist der Ausgangspunkt für ein wirksames BCM. Ein auf Dauer funktionierendes BCM muss als fester Bestandteil in die Unternehmensprozesse integriert werden.

In der Analyse des Geschäftsmodells wird das Verständnis der Unternehmensstrategie dargelegt und zentrale Fragen wie „Was sind die wichtigsten Geschäftsziele der Organisation? Welche Produkte bietet das Unternehmen?“ oder „Wie genau soll die Organisation diese Ziele erreichen?“ beantworten. Die Unternehmensstrategie legt fest, welche Aktivitäten und Vorgänge für den Erfolg des Unternehmens bedeutsam sind und welche nachgeordnet. Alle nachfolgenden Schritte werden von der Unternehmensstrategie und vom Geschäftsprozessmodell abgeleitet.

Mit der Business Continuity-Strategie wird der Rahmen für alle nachfolgenden Maßnahmen des betrieblichen Kontinuitätsmanagements bestimmt. Sie spiegelt die bestmögliche Lösung bei verfügbaren Mitteln wider. Für das BCM ist es bei der Formulierung und Umsetzung entscheidend eine klare und unmissverständliche Leitlinie vorzugeben nach der alle Einzelprojekte, Maßnahmen und technischen Lösungen auszurichten sind.

Das Formulieren einer Vision ist hierbei meist hilfreich und hat das Ziel allen Beteiligten den Nutzen des BCM erkennbar zu machen.

Die Erarbeitung einer umfassenden BCM-Strategie erfolgt in drei wesentlichen Arbeitsschritten (vgl. Abb. 10.3):



Abb. 10.3 Strategische Ebenen im BCM. (Quelle: eigene Darstellung in Anlehnung an von Rössing 2005, S. 130)

- Festlegung der unternehmensweiten BCM-Strategie
- Prozessorientierte Strategie
- Ressourcenorientierte Strategie

Der Zweck der unternehmensweiten BCM-Strategie ist die Vorgabe eines Rahmens und einer dokumentierten BCM-Politik. Die BCM-Strategie bildet das Bindeglied zwischen Geschäftszielen und den zugehörigen BCM-Aufgaben (vgl. von Rössing 2005, S. 130 ff.).

Das Vorgehen in der prozessorientierten Strategie ähnelt stark dem der unternehmensweiten Strategie. Prozesse werden als Bausteine untereinander vergleichbar und jederzeit nachvollziehbar erstellt, um aus Teilstrategien zu unternehmensweiten Vorgaben zu gelangen. Die im Rahmen des BCM erstellten Einzelprozesse müssen, ebenso wie Prozessketten des normalen Prozessablaufes, reibungslos ineinander greifen und als Prozesskette im Krisenfall bestehen. Die prozessorientierte BCM-Strategie beschreibt für jeden Krisenfall die zugehörigen Arbeitsmittel, einzubindenden Personen, benötigte Vorrichtungen und alle anderen notwendigen Elemente, die dem Prozess zur Verfügung stehen müssen. Ziel der ressourcenorientierten BCM-Strategie ist die Auswahl, Priorisierung und Zuweisung der in der Krise begrenzten Ressourcen auf Prozesse.

Verantwortlich für die Festlegung der Strategie ist die oberste Unternehmensführung. Rechenschaftspflichtig ist das mittlere Management, das detaillierte Planungen und Maßnahmen ausführt, überwacht und berichtspflichtig gegenüber der Unternehmensführung ist.

10.2.3 Gefährdungsanalyse, Festlegen des Scope

Zu Beginn eines BCM steht die Betrachtung der Verwundbarkeit und Gefährdung des Unternehmens. Da die Anforderungen zur Absicherung des Kerngeschäfts die Ober- und Untergrenze (verbleibende Restrisiken, mit Investitionen zu vermeidende Risiken) bestimmen, werden die strategischen Vorgaben aus Sicht des Kerngeschäfts bestimmt. Die Übersetzung der Strategie und die klare Darstellung sind entscheidende Erfolgsfaktoren für das Projekt. Bei der Erarbeitung einer BCM-Strategie wird der Top-Down-Ansatz verwendet, um zu einer einheitlichen Strategie auf der Ebene des Gesamtunternehmens zu gelangen (vgl. von Rössing 2005, S. 132). Hierbei kann auch entschieden werden, auf welche Bereiche sich das BCM im Unternehmen erstrecken soll. Unter Umständen ist es von Vorteil erst mit einzelnen, zum Beispiel den wichtigsten Kernbereichen, Organisationsteilen oder Bedrohungen zu beginnen und dann in einem zweiten Schritt den Ansatz weiter auf das ganze Unternehmen auszubreiten und noch fehlende Gefahren abzudecken. Dies ist von der Komplexität, der Größe des Unternehmens aber auch den zur Verfügung stehenden Ressourcen (Personal und Zeit) abhängig.

Ebenfalls muss entschieden werden, auf welche Betrachtungsebene und auf welchen Detailierungsgrad sich das System beziehen soll. Lassen sich für einen einheitlichen Be-

reich wie Technik, Finanzen oder Produktvertrieb schnell einheitliche Kriterien für eine Bewertung schaffen, wird dies bei einer Zusammenfassung aller unternehmensweiten Auswirkungen schwierig und bedarf vorab der prinzipiellen Klärung welcher Analysegrad mit welchem System als Ziel erreicht werden soll.

Das Erstellen guter Analysen bedarf geschulter Moderatoren und Prozesswissen aus den jeweiligen Funktionen und ist nicht beliebig im Unternehmen vorhanden. Von daher macht es durchaus Sinn erst mit den zentralen Risiken aus der Gefahrenanalyse zu beginnen und dann mit Fortschreiten des BCM Lebenszyklus, im Laufe der Jahre, weitere Gefahren mit in das System zu integrieren. Der Scope der jeweiligen Betrachtung muss klar im BCM kommuniziert werden.

10.2.4 Business Impact Analyse

Als nächster Arbeitsschritt folgt die Business Impact Analyse (BIA). Dieser Schritt wird, als alleiniges Element ausgeführt, oft auch als Betriebsunterbrechungsanalyse bezeichnet. Hierbei werden zunächst die Geschäftsbereiche und deren Abhängigkeiten analysiert, um zeitkritische Geschäftsprozesse oder Ressourcen zu identifizieren. Der Zweck besteht darin zu untersuchen, welche Folgen die Ausfälle der jeweiligen Geschäftsprozesse für das Unternehmen nach sich ziehen können. Die Business Impact Analyse (BIA) wird daher oft als das wichtigste und grundlegendste Teilprojekt des BCM-Lebenszyklus bezeichnet. Des Weiteren wird analysiert, wie lange der Ausfall eines Geschäftsprozesses toleriert werden kann, ohne dass dem Unternehmen ein irreversibler Schaden entsteht. Die BIA untersucht alle Auswirkungen, die während und nach einer krisenhaften Situation aus der Sicht des Unternehmens (Bezugssystem) auftreten. Im Wesentlichen identifiziert die BIA potenzielle Schäden, kritische Ressourcen, Anforderungen an den Wiederanlauf sowie weitergehende Auswirkungen von ungeplanten Geschäftsunterbrechungen. Die BIA ist für das Unternehmen eine unerlässliche Voraussetzung, um Schadenspotenziale und Auswirkungen einer Krise festzustellen. Eine BIA ermittelt in der Regel nicht die Eintrittswahrscheinlichkeiten für bestimmte Ereignisse, sondern quantifiziert im Wesentlichen deren Folgen. Eine Ermittlung von Eintrittswahrscheinlichkeiten ist jedoch zumindest für eine Kopplung mit wahrscheinlichkeitsbasierten Modellen des unternehmensweiten Risikomanagements unerlässlich, obwohl streng genommen für das BCM allein gesehen nicht zwingend nötig.

Für eine erstmalige Durchführung einer BIA müssen folgende Voraussetzungen erfüllt sein:

- Definition der Ziele des BCM
- Investitionsbereitschaft in BCM-Lösungen nach erfolgter BIA

Abb. 10.4 BIA-Aufgaben.
 (Quelle: eigene Darstellung in Anlehnung an BSI-Standard 100-4)



Das Ergebnis der Analyse gibt Aufschluss darüber, welche Prozesse und Ressourcen besonders abzusichern sind, damit auch in Krisen und Notfällen die wichtigsten Ziele und Aufgaben der Unternehmung erfüllt werden können.

Abb. 10.4 zeigt die bei einer BIA zu durchlaufenden Schritte.

Anhand der Ergebnisse werden in einem weiteren Schritt die vorhandenen Alternativen zum Umgang mit den Risiken untersucht und vorurteilslos beleuchtet. Die letztlich gewählte Strategie zum Umgang mit einem Risiko ergibt sich aus den zum Zeitpunkt zur Verfügung stehenden Ressourcen, einer Kosten-Nutzenbetrachtung und auch aus bestehenden rechtlichen Vorgaben und ethischen Erwägungen.

Der erste Schritt ist die Analyse des Ist-Zustands. Die dazugehörigen Daten lassen sich meist leicht ermitteln, da sie die tatsächlich vorhandene Situation wiedergeben. Hierzu ist es nötig für die gemäß Scope zu betrachtenden Gefahren Störszenarien zu beschreiben und diese mittels des unternehmensweit vorgegebenen Modells zu bewerten.

Der Soll-Zustand ergibt sich aus den jeweils benötigten Summen aller Wiederanlauf-, Notbetriebs- und Wiederherstellungsanforderungen. Eine Betrachtung des Risikos ist bei

dieser Analyse für das Unternehmen nur dann möglich, wenn für definierte Szenarien sowohl deren Auswirkung (Tragweite) als auch die Wahrscheinlichkeit ermittelt wird, denn nur dann kann sinnvoll entschieden werden, welche Investition oder Maßnahme sinnvoll einzuleiten ist (vgl. GDV 2018). Bedrohungen, Möglichkeiten der Abwendung und Risiken sind für das Unternehmen jedoch nicht statisch, sondern dynamisch und machen eine strategische Bewertung über längere Zeit hinweg nötig. Dies bedeutet aber auch, dass die BIA in regelmäßigen Abständen, bei wesentlichen Änderungen oder nach dem Aufbau neuer Geschäftsfelder immer wieder durchgeführt werden muss. Soll das BCM wesentlicher Bestandteil des Risikomanagements eines Unternehmens sein, dann muss die Analyse aktuell sein. Von daher ist es bei der Planung entscheidend, wie Daten zur Analyse erhoben werden und wieviel Ressourcen zum Betrieb des Systems gebunden werden sollen. Muss zwischen detaillierter aber nur in unregelmäßigen Abständen aktualisierter Analyse oder aktuellem dafür aber weniger detailliertem Datenstand entschieden werden, ist in den meisten Fällen ein sich mit wenig Aufwand aktualisierendes System aufwändiger, detaillierten aber manuellen Systemen vorzuziehen (vgl. von Rössing 2005, S. 136 ff.).

Die Entscheidung über die Einordnung liegt beim Vorstand bzw. bei der Geschäftsführung. Es ist hilfreich einen BCM-Experten heranzuziehen und sich bezüglich der Möglichkeiten beraten zu lassen.

10.2.5 Absicherung der Risiken, Krisenmanagement

Nach der Ermittlung der Risiken wird die Bewertung der Auswirkung durchgeführt. Hierbei spielen vor allem strategische Vorgaben eine Rolle, bzw. es werden aus den Ergebnissen Vorgaben ermittelt. Es lassen sich aber nie alle Risiken in einem Unternehmen absichern, vermeiden oder auf Dritte überwälzen, so dass immer Restrisiken verbleiben. Im Rahmen des BCM ist zu entscheiden, für welche Risikoart sich welche Risikostrategie anwenden lässt. Lässt sich das Problem über Investitionen (verbesserte Technik, Personal) lösen, reicht es die monetäre Auswirkung des Schadens zu versichern oder kann man mit den Risiken leben. Für diese Entscheidung ist eine möglichst realistische Abschätzung der zu erwartenden Kosten/Folgen und der dazugehörigen Eintrittswahrscheinlichkeiten von zentraler Bedeutung, die neben den planbaren operativen Kosten, die durch Controlling und Rechnungswesen betrachtet werden, auch die Kosten aus den Schadenszenarien mit einbezieht. Diese finden sich meist nur in Rückstellungen oder anderen formalen Kostenfaktoren wieder. Im Zusammenhang mit dem BCM wird Investition sehr weitreichend definiert. Zum einen kann eine Investition bedeuten, Gegenstände des Anlage- und Umlaufvermögens im Unternehmen zu erwerben. Andererseits können Ausgaben für die Veränderung von Prozessen, für Versicherungen oder für Outsourcing-Arrangements ebenso als Investition betrachtet werden, wenn sie nachweislich zu einer Veränderung des Schadenpotenzials oder des Gesamtrisikos beitragen (vgl. von Rössing 2005, S. 143). Jede Option bildet einen Baustein in der Kosten-Nutzen-Betrachtung.

Eine wichtige strategische Komponente ist die Einbindung in das unternehmensweite Krisenmanagement. Diese Integration muss lückenlos stattfinden. Da im Falle einer Krise der Krisenstab typischerweise die operative Führung im Unternehmensteil/betroffenen Bereich übernimmt, ist es wichtig einen sinnvollen Schwellenwert festzulegen, ab wann man im Unternehmen von einer Krise spricht. Üblicherweise wird der Schwellenwert aus der BIA-Analyse ermittelt. Zur Abwehr der Krise wird ein Krisenstab vorab definiert und ein Krisenplan für die jeweiligen Szenarien aufgestellt. Der Besetzung des Krisenstabs kommt große Bedeutung zu, da die vom Team getroffenen Entscheidungen in der Krise durch die Leitung akzeptiert werden müssen. Frühwarnsysteme und Sofortmaßnahmen werden erstellt und eingerichtet. Der Umgang mit weitreichenden Krisenzuständen fällt dem Krisenstab im Krisenfall viel leichter, wenn die Auswirkungen auf die Prozesse umfassend bekannt und im Vorfeld untersucht wurden.

Je nach Unternehmen ist es notwendig Lieferanten und Zulieferer mit in die BCM-Strategie einzubinden. Es ist empfehlenswert, nicht nur die Beschaffung, sondern auch das Risikomanagement bei kritischen Ressourcen mit Lieferanten und Dienstleistern zu regeln.

10.2.6 Entwicklung von Kontinuitätsplänen & Umsetzung des Plans

Der normale Betrieb im Unternehmen erfordert kontinuierliches Lernen, zeigt häufige Wiederholungen und basiert auf Erfahrung. Für viele Situationen ist diese Erfahrung im Unternehmen auch für den Notbetrieb vorhanden und muss bei der Erstellung der Kontinuitätspläne für die jeweiligen Szenarien unbedingt mit in die Kontinuitätspläne einfließen. Neben allgemeinen Vorgehensplänen werden auch die in einer Krise benötigten Ressourcen beschrieben. Diese ändern sich oft mit dem Verlauf der Krise und werden in einem zeitlichen Verlauf festgehalten.

Die in der BCM-Strategie festgelegten Ebenen „Unternehmen“, „Prozess“ und „Ressource“ sind allein nicht ausschlaggebend. Eine maßgebliche Rolle bei der Bewältigung einer Krise spielen auch nachfolgende Punkte:

- Personenschäden, Verhalten, gesetzliche Bestimmungen
- Public Relations, Außenwirkung und Wahrnehmung in der Öffentlichkeit
- Verwaltungs- und Administrationstätigkeiten im Unternehmen
- Wirkungen auf verbundene Unternehmen, Kunden und Lieferanten.

Die Kontinuitätsplanung muss hierbei die unterschiedlichen Interessenlagen abdecken. Es müssen gesetzliche Rahmenbedingungen und absolute Werte wie zum Beispiel Gesundheit oder Grundversorgung der Mitarbeiter vorrangig berücksichtigt werden.

Im Vordergrund der Phase steht zunächst die Entwicklung detaillierter Kontinuitätspläne. Die BCM-Strategie dient hierbei bei der Erstellung der Pläne als Leitlinie. Die Kontinuitätspläne beschreiben konkret für jede einzelne Bedrohung, welche einzelnen Schritte und Abwägungen nach Eintreten einer kritischen Situation durchzuführen sind

und wer für die Durchführung verantwortlich ist. Durch die exakte Dokumentation der konkretisierten Lösungen wird der Kontinuitätsplan für das Unternehmen ausführbar gemacht (vgl. Baumann et al. 2018, S. 163 ff.).

Einer der wichtigsten Schritte in dieser BCM-Phase ist zwischen „geschäftskritischen“ und anderen Aktivitäten zu unterscheiden. „Mission critical activities“ sind hierbei Prozesse, die im Krisenfall besonders schnell wiederhergestellt werden müssen, da deren zeitweiliger Ausfall zeitnah zu hohen Schäden führt (vgl. Minister of Public Works and Government Services Canada 2018).

Die meisten Prozesse stützen sich in der Praxis auf eine Vielzahl von technischen, aber auch personellen Ressourcen. Neben der Verkettung von Anlagen und Abläufen im Produktionsprozess kommt der Ermittlung von sogenannten „Bottlenecks“ (Engpassanlagen) in einer Prozesskette entscheidende Bedeutung zu, da ein Ausfall bei diesen Anlagen in der Regel nicht überbrückt werden kann. Gleiches gilt für prozess- und linienübergreifende Hilfsanlagen oder Anlagen/Ressourcen, die über eine zentrale Versorgung wie Energie, Medien oder IT bei einem Ausfall viele oder gar alle Produktionsbereiche und Prozesslinien im Unternehmen betreffen können (vgl. Chubb 2016). Deshalb muss im BCM-Programm zusammen mit Schadenauswirkungen und Abhängigkeiten auch die Ressourcenanforderung an den Normalbetrieb ermittelt werden. Daneben ist auch der Bedarf jeder Ressource für den Notfall zu bestimmen und wie kritisch oder wichtig die jeweilige Ressource für die Fortführung des Betriebs/eingeschränkten Betriebs ist. In der BIA muss zwischen Normalbetrieb und Notbetrieb klar getrennt werden.

Als nächstes folgt die finanzielle Bewertung des Schadens. Sachschäden können anhand von Anlagenlisten mit den betroffenen Vermögenswerten in Bezug auf die Schadenhöhe oft gut ermittelt werden. Die Schwierigkeit besteht darin, vorherzusehen wie groß die Schädigung durch ein Ereignis sein wird und ob diese auch einen finanziellen Verlust durch Betriebsunterbruch oder durch andersartige Folgekosten auslöst. Die Ermittlung der Betriebsunterbrechungskosten als Folge des Verlustes von Prozessleistung ist oft schwierig zu ermitteln, da die finanziellen Einbußen als Funktion der Zeit oft keine eindeutigen Erwartungswerte wie im Falle von reinen Ressourcenverlusten/Sachschäden zulassen. Bei der Ermittlung kommt der verwendeten Methodik zur Bewertung der Risiken große Bedeutung zu. Methoden, die eine Verarbeitung von Ausfall- oder Kostenspannen zulassen, sind in diesem Punkt leichter handhabbar als solche, die nur mit einem Erwartungswert arbeiten. Bei Letzteren muss klar definiert werden, welche Ereignisse (Grad der Schädigung) man für ein Szenario betrachten möchte. Es bietet sich daher bei bedeutenden Szenarien an, diese nach dem Grad der Schädigung/Einwirkung zu unterteilen. Neben dem Ausfall der primären Anlage ist die Auswirkung auf andere Linien im Unternehmen sowie auch auf weitere Standorte und dort verursachte Schäden zu berücksichtigen. Auch kann der Wegfall von zentralen Abnehmern oder Zulieferern große Probleme verursachen. Durch saisonale Abhängigkeiten kann der Zeitpunkt des Schadenereignisses erheblichen Einfluss auf die Schadenhöhe besitzen. Dies ist bei der Bildung der Szenarien zu berücksichtigen.

Ein wichtiger Schritt ist die Bestimmung der maximal tolerierbaren Ausfallzeiten (MTA), der Wiederanlaufzeit (RTO) und der Wiederherstellungszeit. Die MTA bezeichnet die Dauer, nach deren Ablauf die Organisation unwiderruflich Schaden nimmt, falls die kritischen Prozesse für die Lieferung von Gütern bzw. die Erbringung von Dienstleistungen ausfallen. Für ihre Bestimmung wird nur berücksichtigt, welche Auswirkung, also welchen „Impact“, die Unterbrechung eines betrachteten Prozesses hat (vgl. Cornish 2011 S. 130). Der Wiederanlaufpunkt ist in diesem Zusammenhang der Zeitpunkt, an dem die Prozessstabilität soweit erreicht wird, um einen stabilen Notbetrieb mit einer bestimmten Leistung zu gewährleisten. Hierbei muss die Reaktionszeit nach einem Ereignis berücksichtigt werden. Die Reaktionszeit wird für die Mobilisierung von Ressourcen sowie für die Herstellung der notwendigen Bedingungen für den Wiederanlauf und die Wiederherstellung benötigt (vgl. von Rössing 2005, S. 98 ff.). Hinzu kommt das Erfordernis, dass die Funktionalität und die Zweckmäßigkeit der Wiederanlaufumgebung sichergestellt und bestätigt werden muss. Die RTO ist somit eine Größe, die sich verändern und die man zum Beispiel über Erfahrungen aus durchgeführten Notfallübungen verkürzen kann.

Im letzten Schritt wird eine Reihenfolge für den Wiederanlauf und für die Wiederherstellung betroffener Bereiche festgelegt. Diese dient als Landkarte für den Notfallbetrieb und ist die Grundlage für die Weiterentwicklung des BCM.

Wurde bisher bei der BIA im Wesentlichen mit der Tragweite von Bedrohungen gearbeitet, findet im letzten Arbeitsschritt dieser Phase die eigentliche Risikobewertung statt. Sie beschäftigt sich mit der Identifikation der für das Unternehmen wesentlichen Risiken und mit der Ableitung direkter Maßnahmen zur Risikoprävention und Risikobegrenzung im Risikomanagement. Hier besteht auch die Schnittstelle zwischen dem eigentlichen BCM und dem Risikomanagement des Unternehmens.

An dieser Stelle sei noch einmal auf die Notwendigkeit der permanenten/periodischen Aktualisierung der BIA-Analysen hingewiesen. Gerade in jungen, dynamischen Unternehmen kann es schnell zu weitreichenden Änderungen in Geschäftsprozessen und im Kerngeschäft und damit zu veränderten Bedrohungen und Schwachstellen kommen, die im Rahmen der Geschäftsentwicklung unterschiedliche Lösungen für die Abwehr von Krisen nötig machen. Das Prinzip der maximalen Wirkung bei geringstem Aufwand steht auch hier an zentraler Stelle. Nur einfache Systeme, die klar verständlich sind, sich auf die wesentlichen Kernbereiche im Unternehmen fokussieren und auch mit wenig Aufwand an die neue Situation angepasst werden können, haben in den meisten Unternehmen eine Chance auch nach Jahren noch aktuell und zuverlässig zu sein.

Eine weitere zentrale Rolle für das Risikomanagementsystem spielt, wie Risiken im Unternehmen bewertet und vergleichbar gemacht werden. Da letztendlich die monetären Auswirkungen auf das Unternehmen im BCM ausschlaggebend sind, bietet sich die Umrechnung aller Auswirkungen in monetäre Einheiten an.

Bei sehr vielen Bedrohungen kann eine Störung prinzipiell je nach Ausprägung des Störereignisses zu einer kurzen, kleinen oder aber auch zu einer lang anhaltenden, großen Störung führen. So zum Beispiel bei einem Brand an einer kritischen Maschine. Wird das Ereignis frühzeitig erkannt, sind die Folgen gering. Wird das Ereignis zu spät erkannt,

weitet sich der Brand aus und die Folgen sind fatal für das Unternehmen. Von daher stellt sich prinzipiell die Frage, wie man derartige Szenarien betrachten möchte, um ein adäquates BCM und Risikomanagement aufzubauen. Es bieten sich mehrere Methoden an, wie eine Monte-Carlo Simulation, quantifizierbares Rating, qualifiziertes Rating oder rein qualitativ beschreibende Analysen. Die Wahl richtet sich danach, ob die Auswirkungen aus den unterschiedlichen Szenarien miteinander vergleichbar auf einer Skala anhand des Risikos gegenüberstellt und verrechnet werden sollen oder nur in jedem einzelnen Bereich unabhängig voneinander Entscheidungen zur Verbesserung der Situation abgeleitet werden sollen. Systeme zur ganzheitlichen Bewertung aller Risiken im Unternehmen setzen eine differenzierte Betrachtung der Bedrohungen und insbesondere der Wahrscheinlichkeiten für die einzelnen Szenarien voraus. Dies macht die Zusammenführung von BCM und Risikomanagementansatz nötig.

Gerade in größeren Organisationen ist es wichtig einheitliche Arbeitsweisen und für die Analysen verbindliche Methoden vorzugeben und insbesondere zu definieren wie und auf welcher Skala Risiken zu bewerten sind.

Die Umsetzung des BCM führt im Unternehmen schnell zu einer großen Anzahl von periodisch zu aktualisierenden Dokumenten. Der unternehmensweiten Steuerung der Dokumente kommt daher eine große Bedeutung zu und sie unterliegt den allgemeinen Kriterien der Erstellung, Lenkung und Sicherung von Dokumenten.

10.2.7 Test und Aktualisierung des Plans

Das Testen des Plans und seine periodische Aktualisierung und Anpassung an die sich ändernde, aktuelle Unternehmenssituation schaffen die Sicherheit, dass ein Business-Continuity-Plan in der Krise auch tatsächlich funktioniert.

Vielfältige Testverfahren zur Überprüfung der Wirksamkeit des Plans erfordern jedoch sorgfältige Planung und Überwachung und sind teils mit erheblichen Kosten verbunden. Testverfahren sind jedoch notwendig, um den Ist-Zustand zweifelsfrei und unabhängig zu ermitteln und aus den Ergebnissen Stärken und Schwächen des Gesamtkonzepts abzuleiten. Der daraus sich ergebende Handlungsbedarf wird in Wartungsplänen und Maßnahmen umgesetzt.

Das Ziel von Tests und Übungen ist die Feststellung der Funktionstüchtigkeit des BCM-Programms, der Business-Continuity-Pläne, des Krisenmanagements und der allgemeinen Robustheit des Unternehmens gegen Bedrohungen. Da Personen im Unternehmen in der täglichen Praxis mit dem Krisenfall nicht in Berührung kommen, ist es wichtig, das Zusammenspiel der Krisenteams, den Entscheidungsfindungsprozess und die Kommunikation im Team, im Unternehmen und nach außen sowie Verständlichkeit und Interpretation der erstellten Dokumente unter Stress zu testen. Gerade bei international operierenden Unternehmen spielen kulturelle und standortspezifische Unterschiede für die Umsetzung eine bedeutende Rolle.

Durch die erstellte Risikoanalyse, die BIA und das Testprogramm kann herausgefunden werden, ob das bestehende BCM-Programm die Anforderungen an die Krisenreaktion, die Wiederanlauf und die Wiederherstellungszeit erfüllt. Außerdem dient sie der kontinuierlichen Verbesserung des BCM im Sinne der strategischen Ziele (vgl. BCI Good Practice Guide). Sowohl Testkonzept als auch Test- und Übungsgeschehen sollten vollständig dokumentiert werden, damit im Nachgang eine klare Analyse möglich ist. Es bietet sich auch der Einsatz von externen, unabhängigen Beobachtern an.

Im Sinne einer möglichst hohen Flexibilität sollte das Gesamtkonzept aus Tests und Übungen als Baukastensystem aufgebaut werden und auch nur einzeln anhand von konkreten Szenarien oder Bedrohungen getestet werden. Für die Abstimmung mit Vorstand oder Geschäftsführung ist es empfehlenswert, das Testkonzept im Hinblick auf den abgesicherten Schaden und den jährlichen Aufwand zu quantifizieren. Ein Kosten-Nutzen-Vergleich empfiehlt sich.

Der genehmigte Test bedarf meist der Präzisierung der Szenarien, Zeit- und Ressourcenplanung sowie der weiteren Abstimmung mit den Unternehmensbereichen, um zu einer endgültigen und akzeptierten Version zu kommen.

Um möglichst umfassend alle Szenarien zu betrachten, werden die Risikoanalyse sowie die BIA herangezogen. Szenarien lassen sich grob in folgende Kategorien einteilen (vgl. von Rössing 2005, S. 321 f.):

- Zwischenfälle (zeitlich begrenzt, betrifft nur wenige Unternehmensbereiche und fordert in erster Linie Spezialisten)
- Begrenzte Krisen (alle Bereiche betroffen, jedoch erfordern sie aus der Perspektive des Gesamtunternehmens wenig Aufwand)
- Unternehmensweite Krise (das ganze Unternehmen wird zeitweilig behindert/lahmgelegt, alle Bereiche und Managementebenen sind beteiligt)
- Flächendeckende Katastrophen (zeitlich, und räumlich unbegrenzte, nachhaltige Veränderungen des Umfeldes werden vorausgesetzt, Unternehmen ist handlungsunfähig und hat sein Bezugssystem verloren)
- Spezialisierte Szenarien (Teilbereiche werden mit spezifischen Situationen konfrontiert)

Aus jeder Kategorie werden für einen Test realistische und unerwartete Szenarien entwickelt. Für den Entwurf und die Vorbereitung einzelner Testszenarien ist Erfahrung erforderlich. Wenn diese im Unternehmen nicht vorhanden ist, empfiehlt es sich externe Berater einzuschalten.

Nachdem die Szenarien und das Testkonzept feststehen, sollte eine entsprechende Zeit- und Ressourcenplanung aufgestellt werden. Dabei werden Abschätzungen über Vorbereitungs- und Rüstzeiten, Durchlaufzeiten für einzelne Tests und Übungen, Auswertungszeiten und Kommunikations- und Verwaltungsaufwand gemacht. Ebenfalls werden die Ressourcen in vernünftige Sparten gegliedert und entsprechende Aufwände geschätzt.

Die Durchführung des Tests muss konkret überwacht werden. Schwierigkeiten und Probleme während eines Testlaufs müssen abgefangen und bewältigt werden können. Es sollten keine verdeckten Tests und Übungen im Hintergrund durchgeführt werden. Die persönliche Präsenz der Teams steht bei der Durchführung der Tests im Vordergrund. Als personelle Ressourcen werden für die Durchführung ein Kernteam, Testbeobachter, fachliche Mitarbeiter und andere Beteiligte in ihren jeweiligen Rollen benötigt. Vom Kernteam werden zusätzliche Ressourcen wie zum Beispiel Büroräume, Telekommunikation und vorgesehene Hilfsmittel gemäß Plan benötigt. Für die Überwachung werden mindestens ein Testleiter, verschiedene Beobachtergruppen sowie ein oder mehrere Protokollanten eingesetzt.

10.2.8 Revision

Das Business Continuity Management ist auch Gegenstand der internen und externen Revision. Einerseits berücksichtigt die interne Revision die Vorschriften zu Corporate Governance und andererseits den Wunsch der Unternehmensleitung nach Ordnung und Kontrolle. Im Grundsatz gilt hier das Vieraugenprinzip: Eine Überprüfung der Sachverhalte durch eine unabhängige Person. Sie bringt zusätzliche Sicherheit und erlaubt eine unvoreingenommene Auseinandersetzung mit Problemen und notwendigen Maßnahmen. Zu Beginn der Revision sind die Prüfungsziele abzustimmen. Diese sind:

- Jahresabschluss;
- Prüfungen von Sonderthemen beziehen sich auf den Jahresabschluss und gegebenenfalls auf das bilanzielle Risiko. An der Schnittstelle zwischen BCM und Jahresabschluss stehen konkrete Zahlen und nicht eine Abwägung im Vordergrund;
- Einhaltung der Gesetze im Rahmen der Revision.

Die Qualität eines Prüfgegenstandes, eines Managementprogramms oder der BCM-Fähigkeit sind selten Gegenstand dieser Prüfung, da es sich hierbei meist um prozessbezogene Prüfungen handelt (vgl. von Rössing 2005, S. 348 ff.).

Der Prüfer untersucht ausschließlich die Erfüllung der vorgegebenen Mindestanforderungen. Die Ausgangslage des Unternehmens ist die Grundlage für alle Prüfstrategien und nachfolgenden Prüfungshandlungen. Hinsichtlich durchgeföhrter Audits wird zwischen internen und externen Audits unterschieden. Ein externer Auditor kann beispielsweise auch der eigene Sachversicherer sein. Ein externes Audit soll feststellen, ob die Anforderungen der Organisation an ein BCM erfüllt werden und ob der Business-Continuity-Plan schlüssig und nachvollziehbar ist. Anforderungen an interne Audits sind in vielen Unternehmen festgelegt. Hierbei unterscheiden sich Durchführung, Form und Dokumentation nicht von den üblicherweise zu anderen Fragestellungen im Unternehmen durchgeföhrten Audits oder Revisionen (vgl. GDV, S. 15). Umfang und Ziele der Revision richten sich

nach dem Reifegrad des Unternehmens sowie der grundlegenden Fragestellung. Die Auditkriterien sind vorab festzulegen.

10.2.9 Auswertung und Verbesserung

Auswertung und Aktualisierung der Pläne sind Kernbestandteile der Weiterentwicklung des BCM-Programms. Da Unternehmen hinsichtlich der Geschäftsentwicklung, den Prozessen sowie der Organisationsstruktur ständig dem Wandel ausgesetzt sind, bezieht sich die Verbesserung oder Anpassung des Programms nicht zwingend auf Fehler im System, sondern oft auf die Anpassung an die neue, geänderte Situation. Auswertung bedeutet, die Ergebnisse der Analyse zusammenzustellen, um Fehler oder Mängel im System aufzudecken. Verbesserung zielt darauf ab, das BCM an die geänderten Anforderungsprofile der Geschäftsprozesse anzupassen. Die Trennung ist auch aus bilanzieller Sicht empfehlenswert, da Reparaturen anders bewertet werden als Upgrades. Genauso wie bei der Durchführung von Tests und Übungen, sind Auswertung und Verbesserung zu dokumentieren.

Im ersten Schritt werden Auswertungszyklen festgelegt. Sie sind Grundlage für die BCM-Strategie. Die Auswertungszyklen sind ein Teil des BCM-Gesamtbudgets und müssen entsprechend in die Strategie und das Investitionsverhalten des Unternehmens integriert werden. Eine Kosten-Nutzen-Betrachtung ist sinnvoll. Grundsätzlich sollten Auswertungen und Aktualisierungen in einem jährlichen Intervall stattfinden. Dabei sind folgende Punkte zu berücksichtigen:

- Risikobewertung und BIA
- BCM-Strategie und Dokumentation
- Kontinuitätspläne
- Stand der BCM-Kultur und Anpassung der Unternehmensziele
- Ausbildungsprogramm
- Testplanung für nachfolgende Beobachtungszeiträume

Die Betrachtung der jährlichen Auswertung ist abteilungsübergreifend durchzuführen. Unterjährige Auswertungen können nach kritischen Ereignissen durchaus sinnvoll sein.

Änderung von Kontinuitätsplänen und die Freigabe und Verteilung geänderter Dokumente sollten zeitnah erfolgen, damit das BCM immer auf dem neusten Stand ist.

Zudem ist ein regelmäßiges Management-Review der BCM-Strategie durchzuführen. Hierbei sollte geprüft werden, ob die Leitlinien und Zielsetzungen des BCM noch stimmig und aktuell sind. Geänderte Fertigungsprozesse, geänderte Fertigungsverfahren, geänderte Lieferanten oder geänderte Gesetze und Vorschriften werden im Verbesserungsprozess aufgedeckt (vgl. GDV, S. 15 f.).

10.3 Fazit

Das BCM stellt ein Rahmenwerk für die Verbesserung der Widerstandsfähigkeit eines Unternehmens gegen Risiken bereit und bietet die Möglichkeit, die Interessen der Stakeholder, die Reputation, die Marke und die Wertschöpfung zu sichern. Durch Vorbereitung des Unternehmens und die getroffenen Maßnahmen wird eine Krise leichter und mit weniger negativen Auswirkungen überwunden werden können. Gleichzeitig ist durch die Identifikation aktueller und zukünftiger Bedrohungen eine detaillierte und genaue Analyse der Unternehmensrisiken möglich. Der größte Vorteil im BCM liegt in der aktiven Minimierung der Auswirkung von Störereignissen, insbesondere in der Minimierung der Ausfallzeiten und damit der Reduktion entstehender Kosten im Schadenfall. Des Weiteren gewährleistet das BCM durch die getesteten Prozesse auch im Krisenfalle eine systematische Durchführung der wichtigsten Aufgaben im Unternehmen bei eingeschränkter Verfügbarkeit der Ressourcen.

Ohne Vorwissen ist es in größeren Organisationen meist sehr schwer ein gutes und stabiles BCM aufzubauen. Von daher sind in der Praxis erfahrene, langjährig beschäftigte Mitarbeiter im BCM-Team sowie ein geschulter Business Continuity Manager sehr hilfreich, wenn nicht Voraussetzung für die Erstellung eines fundierten BCM.

Die Einführung eines BCM ist meist mit hohen Kosten verbunden, da es einerseits in der Durchführung ein sehr ressourcenintensives Projekt darstellt und andererseits in der Folge zur Verbesserung der Risikosituation in Personal, Ressourcen, IT und andere Bereiche investiert wird. Einige Kostenpositionen sind zudem fortlaufend, wie zum Beispiel Personalkosten sowie Kosten für die regelmäßige Prüfung und Aktualisierung des BCM. Die Aktualisierung des BCM ist allerdings zwingend erforderlich und alternativlos, um dem Management ein Instrument in die Hand zu geben, die veränderte Risikolandschaft des Unternehmens zu monitoren und gezielt auf eine Veränderung und Risiken zu reagieren. Von daher ist das BCM, trotz Kosten und Bindung von Ressourcen im Unternehmen, eine Investition, um die Zukunftsfähigkeit und die Stabilität des Unternehmens abzusichern.

Literatur

- Baumann, S., et al. (2018). Business Continuity Management – unverzichtbares Element eines angemessenen Risikomanagements. In S. Hunziker & J. O. Meissner (Hrsg.), *Ganzheitliches Chancen- und Risikomanagement* (S. 163–192). Wiesbaden: Springer Gabler.
- Bergauer, A. (2003). *Führen aus der Unternehmenskrise*. Berlin: Erich Schmidt.
- BSI – (2008). Standard 100-4 Notfallmanagement Version 1.0.
- Chubb. (2016). To the point business continuity planning.
- Cornish (2011). Busines continuity management methodology. In A. Hiles (Hrsg.), *The definitive handbook of business continuity management* (3. Aufl., S. 121–136). Chichester: Wiley.
- Gesamtverband der Deutschen Versicherer GDV. (2018). Business Continuity Management Hinweise für Unternehmen.

- International Organization for Standardization. (2012). ISO-Norm 22301:2012.
- Krystek, U. (1987). *Unternehmenskrisen: Beschreibung, Vermeidung und Bewältigung überlebenskritischer Prozesse in Unternehmungen*. Wiesbaden: Springer Gabler.
- Minister of Public Works and Government Services Canada. (2018). A guide to business continuity planning.
- Müller, A.-L. (2014). Business Continuity Management bei Finanzdienstleistungsunternehmen. *HMD – Praxis der Wirtschaftsinformatik*, 51, 339–349.
- Spörrer, S. (2014). *Business Continuity Management, ISO 22301 und weitere Normen im Rahmen der Informationstechnologie*. Köln: Kölner Wissenschaftsverlag.
- Von Rössing, R. (2005). *Betriebliches Kontinuitätsmanagement*. Bonn: mitp.

Marco Mirkes studierte Geoökologie an der Universität Bayreuth und arbeitet seit mehr als 25 Jahren im Bereich Risikobewertung, Schadenverhütung und Risk Management von Industrieunternehmen bei Versicherungsunternehmen. Im Laufe seines Berufslebens war er sowohl in den verschiedensten Risikobereichen als auch in unterschiedlichen Funktionen in diesem Arbeitsgebiet tätig. Neben beratenden Tätigkeiten hat er auch verantwortlich bei der Implementierung eines Business Continuity Management Systems im eigenen Hause mitgewirkt. Zur Zeit leitet Herr Mirkes den Bereich Risk Engineering and Loss Prevention der Generali Global Corporate & Commercial in Deutschland.

Emine Özcan studierte Versicherungswesen mit den Schwerpunkten Risikomanagement, Bilanzierung von Versicherungsunternehmen und Daten- und Organisationvermittlung im dualen System mit der AXA Versicherung AG zusammen am Institut für Versicherungswesen der Technischen Hochschule Köln. Im Anschluss absolvierte sie dort auch das Masterstudium Risk & Insurance.



Zertifizierung von Risikomanagementsystemen und -prozessen

11

Olaf Seiche und Erik Klaedtke

Zusammenfassung

Die mögliche Zertifizierung von Risikomanagementsystemen. Zu Beginn werden die Grundlagen der Zertifizierung und Auditierung mit Blick auf die Managementsysteme einer Organisation vermittelt. In diesem Zusammenhang wird die Motivation von Unternehmen zur Durchführung einer Auditierung bzw. Zertifizierung aufgezeigt. Ergänzend dazu werden aktuelle Themen und Trends rund um die Zertifizierung von Managementsystemen dargestellt. Ein wichtiger Bestandteil eines Managementsystems ist das Risikomanagement. Gerade in der heutigen Zeit existieren immer mehr Risiken. Daher sind Standards, Leitlinien und Normen für den Umgang und die Behandlung von Risiken unerlässlich. Organisationen können mit einer Zertifizierung der Risikomanagementsysteme sich selbst und auch externen Parteien aufzeigen, wie gut ihr Risikomanagementsystem funktioniert. Gerade für den Bereich der Industriever sicherung kann eine Zertifizierung viele Informationen darlegen, die zum Beispiel ein Underwriter gar nicht erhalten und somit für die Risikoeinschätzung nicht nutzen kann.

O. Seiche (✉)

TÜV Rheinland Cert GmbH, Köln, Deutschland

E-Mail: olaf.seiche@de.tuv.com

E. Klaedtke

TH Köln, Institut für Versicherungswesen, Köln, Deutschland

E-Mail: erik.klaedtke@outlook.com

11.1 Einleitung

Im Jahr 2017 haben sich über 1,5 Millionen Unternehmen zertifizieren lassen. Gerade Managementsysteme, wie das Qualitäts- oder Umweltmanagement, werden am häufigsten zertifiziert. (vgl. International Organization for Standardization 2018). Dabei spielen die Normen *DIN EN ISO 9001* (Anforderungen an Qualitätsmanagementsysteme) und *DIN EN ISO 14001* (Anforderungen an Umweltmanagementsysteme) eine wichtige Rolle.

Neben den beiden häufigsten zertifizierten Managementsystemen ist das betriebliche Risikomanagement ein wichtiger Bestandteil. Heutzutage gibt es mehr Risiken als je zuvor. Die Unternehmen fürchten vor allem einen Konjunkturrückgang/einen langsamem Aufschwung, Schädigungen der Reputation und des Markenimages sowie zunehmende Veränderungen der Marktfaktoren. Um diesen Risiken gerecht zu werden, ist ein funktionierendes Risikomanagement unerlässlich. Ungefähr zwei Drittel aller Unternehmen haben einen Unternehmensbereich, der sich mit dem Thema Risikomanagement beschäftigt (vgl. Aon plc. 2019).

Um den wachsenden Anforderungen an das betriebliche Risikomanagement gerecht zu werden, haben Unternehmen/Organisationen die Möglichkeit, sich ihr Risikomanagementsystem (und -prozesse) auditieren und durch eine externe (akkreditierte) Gesellschaft zertifizieren zu lassen.

In diesem Kapitel wird sich spezifisch mit der Zertifizierung von Risikomanagementsystemen und -prozessen auseinandergesetzt. Kerntypen werden die Zertifizierung als solches, die Wirksamkeitsüberwachung von Risikomanagementsystemen und der zertifizierte Risikomanager sein.

Der erste Abschnitt befasst sich mit den Grundlagen der Zertifizierung und Auditierung. Dabei wird zum einen die Motivation für eine Zertifizierung und deren Zielsetzung näher beleuchtet. Zum anderen werden aktuelle Trends und Themen rund um die Zertifizierung von Managementsystemen betrachtet. Nachfolgend werden die unterschiedlichen Normen und Leitlinien kurz vorgestellt, um sich danach mit den Zertifizierungsunternehmen und deren Akkreditierung zu befassen.

Im zweiten Abschnitt wird sich detaillierter mit der Zertifizierung von Risikomanagementsystemen und -prozessen auseinandergesetzt. Als Grundlage für standardisierte Managementsysteme wird die *DIN EN ISO 9001* (Anforderungen an das Qualitätsmanagementsystem) näher beleuchtet. Im Anschluss werden die Leitlinien für das Risikomanagementsystem einer Organisation detailliert betrachtet. Zusätzlich werden der Ablauf einer Zertifizierung sowie die Wirksamkeitsüberwachung dargestellt. Abschließend wird exemplarisch die Zertifizierung der FERMA für Risikomanager aufgezeigt.

Zum Schluss wird im Fazit die Relevanz von zertifizierten Risikomanagementsystemen und -prozessen im Zusammenspiel mit dem betrieblichen Risikomanagement und der Industriever sicherung herausgestellt.

11.2 Zertifizierung und Auditierung

Im Allgemeinen wird zwischen einer Zertifizierung und einer Auditierung unterschieden. Das Wort „Audit“ stammt von dem lateinischen Wort „audire“ ab, was so viel wie „hören“ bedeutet. Im Englischen bedeutet „audit“ „Anhörung“ oder „Überprüfung“. Diese erste Annäherung an den Begriff „Audit“ geht durchaus in die Richtung der Definition nach dem Leitfaden zur Auditierung von Managementsystemen (*DIN EN ISO 19011*). In diesem wird ein Audit als ein systematischer, unabhängiger und dokumentierter Prozess zur Erlangung von objektiven Nachweisen und zu deren objektiver Auswertung zur Ermittlung des Erfüllungsgrades der Auditkriterien beschrieben (vgl. DIN Deutsches Institut für Normung e. V. 2018b, S. 11).

Bei einer Zertifizierung (eines Managementsystems) handelt es sich um eine spezielle Form eines Audits, um ein Drittparteien-Audit, also ein externes Audit (vgl. Brauweiler et al. 2015, S. 27). Hierbei erhält die auditierte Organisation durch eine akkreditierte Stelle einen Nachweis über die Konformität ihres Managementsystems mit der jeweils zugrunde liegenden Norm (vgl. Brauweiler et al. 2015, S. 7).

In diesem Kapitel werden die allgemeinen Grundsätze der Zertifizierung und Auditierung von Managementsystemen nähergebracht. Im Anschluss werden die verschiedenen Normen und Leitlinien, die zu auditieren und zertifizieren sind, vorgestellt. Darauf aufbauend wird sich mit den verschiedenen Zertifizierungsunternehmen und deren Akkreditierung auseinandergesetzt.

11.2.1 Allgemeine Grundsätze

Um später vertieft in die Zertifizierung von Risikomanagementsystemen eingehen zu können, ist es von Relevanz einen allgemeinen Überblick über die Grundsätze von Audits und Zertifizierungen von Managementsystemen zu erhalten. Dabei spielen vor allem die Motivation und Zielsetzung zur Durchführung von Audits/Zertifizierungen eine wichtige Rolle. Zudem werden aktuelle Trends im Bereich Zertifizierung aufgezeigt.

11.2.1.1 Motivation und Zielsetzung für die Auditierung und Zertifizierung von Managementsystemen

„Audits spielen bei der Umsetzung von Managementsystemen eine wichtige Rolle, denn es soll durch sie regelmäßig geprüft werden, ob die Prozesse einer Organisation geeignet sind, die an sie gestellten Anforderungen zu erfüllen“ (Brauweiler et al. 2015, S. 3). Diese Anforderungen können sich zum Beispiel aus Normen, aus Unternehmensstrategien, Gesetzen, Standards oder auch Kundenanforderungen ergeben. Die Zielsetzung zur Durchführung von Audits hängt stark von den unterschiedlichen Arten von Audits ab.

Die *DIN EN ISO 19011* (Leitfaden zur Auditierung von Managementsystemen) unterscheidet zwischen drei verschiedenen Arten von Audits (vgl. DIN Deutsches Institut für Normung e. V. 2018b, S. 11 f.).

- **Erstparteien-Audit:** Dies sind sogenannte interne Audits, bei denen die Organisation Audits selbst durchführt oder in ihrem Auftrag durchgeführt werden.
- **Zweitparteien-Audit:** Hier werden die Audits von externen Parteien durchgeführt oder in deren Auftrag durchgeführt, die ein Interesse an der Organisation habe. Dies können zum Beispiel Kunden sein.
- **Drittparteien-Audit:** Bei dieser externen Audit-Art werden die Audits von unabhängigen Organisationen, wie zum Beispiel akkreditierte Zertifizierungsorganisationen oder staatliche Behörden, durchgeführt.

Hierbei lässt sich durchaus erkennen, dass die Motivation zur Durchführung von Audits entweder durch interne oder externe Interessen getrieben ist. Bei internen Audits (Erstparteien-Audit) kann überprüft werden, ob zum Beispiel Prozesse, Systeme oder Produkte den gestellten Anforderungen, die sich von Unternehmensstrategien, Gesetzen, Standards oder Kundenbedürfnissen ableiten, gerecht werden. Hieraus kann das Management weitere Maßnahmen zur Optimierung der Organisation ableiten. Externe Audits (Zweit- und Drittparteien-Audits) hingegen sind durch die Interessen von Parteien außerhalb der Organisation getrieben. Bei einem Zweitparteien-Audit kann der Auftraggeber direkt auf Nicht-Konformitäten und Verbesserungspotenziale hinweisen und auf Korrekturmaßnahmen einwirken. Durch die Durchführung eines Drittparteien-Audits, wie zum Beispiel einem Zertifizierungsaudit, erlangt die auditierte Organisation einen Nachweis über die Konformität eines (Management-)Systems mit einer zugrunde liegenden Norm durch eine akkreditierte dritte Partei (vgl. Brauweiler et al. 2015, S. 6 f.).

In der wirtschaftswissenschaftlichen Theorie lässt sich das Vorhandensein von Zertifizierungen durch das Nicht-Funktionieren des Marktes erklären. Die Konsumenten verfügen nicht, wie angenommen, über die vollkommenen Informationen über die Preise und Qualität eines Produktes. Die Konsumenten sind daher nicht bereit das angebotene Produkt für den angegebenen Preis zu kaufen, da sie nicht wissen, dass der Preis der Qualität des Produktes entspricht. Daher werden keine Produkte mehr mit hoher Qualität angeboten. Die Konsumenten senken nun ihre Qualitätsanforderungen an das Produkt. Jedoch sind sie jetzt immer noch nicht bereit den geforderten Preis für die angebotenen Produkte mit mittlere Qualität zu zahlen, da sie immer noch nicht wissen, ob das Preis-Leistungs-Verhältnis stimmt. Also nimmt der Anbieter ebenfalls seine Produkte vom Markt. Dieser Prozess wiederholt sich so lange bis nur noch Produkte mit einer sehr geringen Qualität vorhanden sind. Es kommt also zu einem Preis- und Qualitätsverfall im Markt.

Ein Mittel auf Seiten der Anbieter zum Abbau der Informationsasymmetrie im Markt sind Zertifizierungen, die dem Kunden signalisieren, dass die Qualität des Produktes hoch ist und der verlangte Preis gerechtfertigt ist. So kann der Konsument Produkte mit hoher Qualität von Produkten mit niedriger Qualität unterscheiden (vgl. Friedel und Spindler 2016, S. 25).

Die Zielsetzung einer Zertifizierung leitet sich hauptsächlich von der Motivation der Unternehmen zur Durchführung einer Zertifizierung ab. Die größte Motivation der Unter-

nehmen ist der Qualitätsnachweis gegenüber externen, dritten Parteien. Dieser Nachweis kann vor allem den Abnehmern der Produkte als auch dem Gesetzgeber gegenüber erbracht werden. Der Gesetzgeber ist hauptsächlich an der Sicherstellung eines einheitlichen Sicherheits- und Qualitätsniveaus interessiert. Die Unternehmen hingegen erhoffen sich von einer Zertifizierung sogenannte unternehmensinterne und unternehmensexterne Effekte.

Die Motivation für eine Zertifizierung ist größtenteils durch externe Faktoren getrieben. Die wichtigsten externen Effekte sind vor allem die Einhaltung von gesetzlichen Bestimmungen, die Einhaltung von Kundenanforderungen und der erleichterte Zugang zu in- und ausländischen Märkten. Der für die Unternehmen relevanteste interne (Neben-) Effekt ist die Verbesserung von Prozessen (vgl. Friedel und Spindler 2016, S. 28 f.). Dies deckt sich vor allem mit der Zielsetzung von Audits ab.

Grundsätzlich ist zu erkennen, dass ein (externes) Zertifizierungsaudit häufig deswegen durchgeführt wird, weil der Markt es zu Teilen verlangt. Würden keine gesetzlichen Vorgaben bestehen oder die Kundenanforderungen es nicht verlangen, so würden die zertifizierten Organisationen eher Erst- oder Zweitparteien-Audits durchführen.

11.2.1.2 Zertifizierung von Managementsystemen in der heutigen Zeit

Wie schon in den vorherigen Kapiteln benannt, spielt die Zertifizierung von Managementsystemen eine immer wichtiger werdende Rolle. Die Gründe dafür sind vielfältig.

In Tab. 11.1 ist die Anzahl an Zertifizierungen nach den wichtigsten ISO Management-system-Standards in den Jahren 2015 bis 2017 dargestellt. Insgesamt lässt sich ein geringer Rückgang verzeichnen. Dies liegt hauptsächlich am Rückgang der Zertifizierungen nach der DIN EN ISO 9001. Nach Angaben der International Organization for Standardization liegt dies an den rückläufigen Zahlen in Deutschland und Italien. Diese rückläufigen

Tab. 11.1 Weltweite Anzahl der Zertifizierungen nach Managementsystem-Standards (vgl. International Organization for Standardization 2018)

	Anzahl 2015	Anzahl 2016	Anzahl 2017	Veränderung (%) 2016 zu 2017
DIN EN ISO 9001	1.034.180	1.105.937	1.058.504	-4,29 %
DIN EN ISO 14001	319.496	346.147	362.610	+4,76 %
DIN EN ISO/IEC 27001	27.536	33.290	39.501	+18,66 %
DIN EN ISO 22000	32.056	32.139	32.722	+1,81 %
DIN EN ISO 13485	26.255	29.585	31.520	+6,54 %
DIN EN ISO 50001	11.985	20.216	21.501	+6,36 %
DIN 20000-1	2778	4537	5005	+10,31 %
DIN EN ISO 22301	3113	3853	4281	+11,11 %
ISO 39001	k.A.	478	620	+29,71 %
DIN 28000	k.A.	356	494	+38,76 %
Gesamt	1.457.399	1.576.538	1.556.758	-1,25 %

figen Zahlen lassen sich jedoch auf eine zum Vorjahr abweichende Erhebungsmethode zurückführen. Daher sind diese Werte nicht mit den Vorjahreswerten zu vergleichen. Daher lässt sich klar erkennen, dass die Gesamtanzahl an Zertifizierungen von Managementsystemen weltweit zunimmt. Dies zeigt auch, dass die Zertifizierung von Managementsystemen in Organisationen immer wichtiger wird.

Dies wird ebenfalls in der Anzahl der Managementsystem-Standards deutlich. Momentan gibt es 59 Normen- und Leitlinien, die von der ISO veröffentlicht wurden (vgl. International Organization for Standardization ([o. J.](#))). Die ISO verfolgt das Ziel, dass alle Managementsystemnormen und Leitlinien nach einer einheitlichen Struktur und nach gleichartigen Kerninhalten aufgebaut sind. Dafür wurde die sogenannte High-Level-Structure (HLS) eingeführt. Mit der HLS sollen die Angleichungen der unterschiedlichen Normen verbessert werden. Zudem dient sie als Leitfaden zur Entwicklung zukünftiger Normen. Langfristig sollen alle Normen und Leitlinien die gleiche übergeordnete Gliederung und gemeinsame Kernanforderungen enthalten.

Die Struktur der HLS besteht aus zehn Kapiteln. Je nach Norm fallen spezifische Unterkapitel an.

1. Anwendungsbereich
2. Normative Verweisungen
3. Begriffe
4. Kontext der Organisation
5. Führung
6. Planung
7. Unterstützung
8. Betrieb
9. Bewertung der Leistung
10. Verbesserung

Mit der HLS werden die Normen und Leitlinien für die Anwender verständlicher. Dadurch, dass die Begriffe, Definition etc. vereinheitlicht werden und der Aufwand bei der Dokumentation sinkt, wird die Einführung mehrerer Managementsysteme gleichzeitig (zum Beispiel Qualitätsmanagement und Umweltmanagement) wesentlich vereinfacht und effizienter. So lassen sich auch weitere Managementsysteme schneller in vorhandene Systeme integrieren. Die bei integrierten Managementsystemen anfallenden internen Audits können dadurch gleichzeitig durchgeführt werden. So lassen sich Synergien nutzen (vgl. DQS GmbH ([o. J.](#))).

Von den momentan 59 vorhandenen Managementstandards wurden 23 nach der High Level Structure aufgebaut (vgl. International Organization for Standardization ([o. J.](#))).

11.2.2 Managementsysteme: Normen und Leitlinien

Das Managementsystem einer Organisation beschäftigt sich mit der systematischen und geplanten Herangehensweise an die Umsetzung der Unternehmensstrategie. Mit ihnen soll eine ganzheitliche Unternehmenspolitik zur Erreichung der Ziele geschaffen werden.

Die unterschiedlichen Teilsysteme liefern eine methodische Unterstützung bei der Gestaltung der Prozesse. Ein Großteil der Teilmanagementsysteme ist durch die ISO Managementstandards standardisiert. In diesen Standards werden die Anforderungen an das jeweilige Managementsystem dargelegt. Hier nun ein Auszug der bekanntesten Normen und Leitlinien:

- DIN EN ISO 9001: Qualitätsmanagementsysteme – Anforderungen
- DIN EN ISO 14001: Umweltmanagementsysteme – Anforderungen mit Anleitung zur Anwendung
- DIN EN ISO/IEC 27001: Informationstechnik – Sicherheitsverfahren – Informations-sicherheitsmanagementsysteme – Anforderungen
- DIN ISO 31000: Risikomanagement – Leitlinien
- DIN ISO 45001: Managementsysteme für Sicherheit und Gesundheit bei der Arbeit – Anforderungen mit Anleitung zur Anwendung
- DIN EN ISO 50001: Energiemanagementsysteme – Anforderungen mit Anleitung zur Anwendung

Der am weitesten verbreitete Managementsystemstandard ist die *DIN EN ISO 9001*. Viele Organisationen legen Wert darauf, dass potenzielle Geschäftspartner nach der *DIN EN ISO 9001* zertifiziert sind, bevor sie eine Geschäftsbeziehung mit ihnen eingehen. In dieser Norm werden die Anforderungen an das Qualitätsmanagementsystem einer Organisation dargestellt. Sie gilt häufig als Ausgangspunkt für die Zertifizierung weiterer Managementsysteme.

In Abb. 11.1 der ISO kann man erkennen, wie die unterschiedlichen Management-systemstandards (MSS) zusammenspielen. Hierbei wird zwischen den allgemeinen

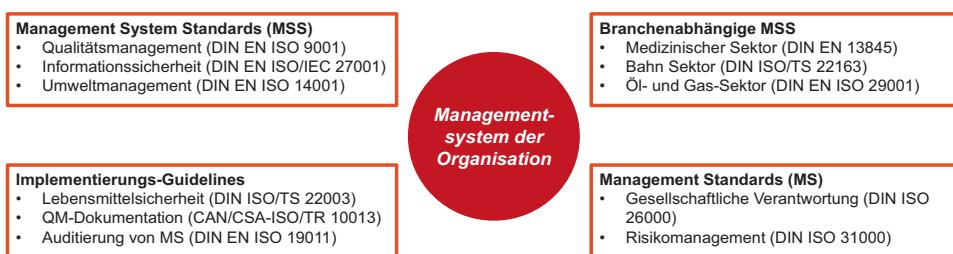


Abb. 11.1 Managementsystem Standards. (Quelle: eigene Darstellung in Anlehnung an International Organization for Standardization)

MSS und branchenspezifischen MSS unterschieden. Die allgemeinen MSS können branchenunabhängig eingesetzt werden. Häufig sind diese Standards anhand der HLS aufgebaut. Hierzu zählen die beiden bekanntesten MSS, die *DIN EN ISO 9001* (Qualitätsmanagement) und die *DIN EN ISO 14001* (Umweltmanagement). Die branchenspezifischen MSS sind häufig nur in bestimmten Branchen anwendbar, wie zum Beispiel im medizinischen Bereich (*DIN EN ISO 13485*) oder im Öl und Gas Sektor (*DIN EN ISO 29001*).

Des Weiteren gibt es unterstützende Standards und Leitlinien. Diese beziehen sich häufig auf einen anderen Standard oder stellen die Anforderungen an die Durchführung der Zertifizierung nach einer Norm, wie zum Beispiel die *DIN EN ISO 19011* (Leitfaden zur Auditierung von Managementsystemen), dar.

Ergänzt werden die MSS durch Management Standards. Diese Standards beinhalten weitestgehend Leitlinien/Richtlinien für die Ein- und Durchführung von Managementsystemen. Hierunter fallen unter anderem die Risikomanagement Leitlinien (*DIN ISO 31000*). Das Besondere ist, dass man nach dieser Norm nicht zertifiziert werden kann. Die *DIN ISO 31000* nennt lediglich Leitlinien für das Risikomanagement in einem Unternehmen und stellt keine Anforderungen an das Risikomanagementsystem an sich. Für die Zertifizierung wird daher häufig die österreichische Norm *ONR 49001* (Risikomanagement für Organisation und Systeme – Risikomanagement – Umsetzung von ISO 31000 in die Praxis) genutzt.

Grundsätzlich gibt es keinen Zwang Normen und Leitlinien anzuwenden. Erst durch einen Verweis von EU-Richtlinien oder nationalen Gesetzen erlangen Normen eine Rechtsverbindlichkeit. Neben dieser direkten Rechtsverbindlichkeit wird ebenfalls von einer indirekten Rechtsverbindlichkeit gesprochen. Häufig werden bei gerichtlichen Streitfällen Normen und Leitlinien als Entscheidungshilfe herangezogen, zum Beispiel in Haftungsprozessen. Dadurch, dass in den Normen und Leitlinien die Anforderungen an Prozesse und (Management-)Systeme nach dem aktuellen Stand der Technik und des Wissens erstellt werden, können diese bei der Beurteilung, ob zum Beispiel eine beklagte Vertragspartei in einem Haftungsprozess den allgemeinen anerkannten Stand der aktuellen Technik beachtet hat und somit der verkehrsüblichen Sorgfalt nachgekommen ist, herangezogen werden. Im Umkehrschluss kann die Nicht-Anwendung von Normen in bestimmten Rechtsgebieten als grob fahrlässiges Handeln gesehen werden kann. So mit erhalten manche Normen eine indirekte Rechtsverbindlichkeit.

11.2.3 Zertifizierungsunternehmen und deren Akkreditierung

Eine Zertifizierung von Managementsystemen darf prinzipiell von jeder beliebigen Organisation durchgeführt werden. Es gibt keine gesetzliche Regelung, die verlangt, dass bestimmte Voraussetzungen für die zertifizierende Organisation erfüllt sein müssen.

In Deutschland gibt es eine Vielzahl von Unternehmen, die sich mit der Zertifizierung von Normen, Leitlinien und anderen Standards auseinandersetzen. Die Unternehmen unterscheiden sich vor allem in dem Punkt der Akkreditierung. Für Zertifizierungsstellen besteht die Möglichkeit, dass sie sich durch die nationale Akkreditierungsstelle der Bundesrepublik Deutschland, die *Deutsche Akkreditierungsstelle GmbH (DAkkS)*, akkreditieren lassen.

In der *DIN EN ISO/IEC 17011* (Anforderungen an Akkreditierungsstellen) ist die Akkreditierung wie folgt definiert: Bei einer Akkreditierung bestätigt eine dritte Seite formal, dass eine Konformitätsbewertungsstelle (KBS) die Kompetenz besitzt, bestimmte Konformitätsbewertungsaufgaben durchzuführen. Eine KBS führt Konformitätsbewertungstätigkeiten durch (vgl. DIN Deutsches Institut für Normung e. V. 2018a, S. 9). Nach der *DIN EN ISO/IEC 17021-1* (Konformitätsbewertung) handelt es sich bei einer Zertifizierung von Managementsystemen um eine solche Konformitätsbewertungstätigkeit durch Dritte. Folglich handelt es sich bei Stellen, die solche Dienstleistungen anbieten (Zertifizierungsstellen), um KBS (vgl. DIN Deutsches Institut für Normung e. V. 2015, S. 9).

In Deutschland fällt die Akkreditierung von KBS in den hoheitlichen Aufgabenbereich des Staates. Die schon eben angesprochene DAkkS handelt nach der Verordnung (EG) Nr 765/2008 und dem Akkreditierungsstellengesetz (AkkStelleG) im öffentlichen Interesse als alleiniger Dienstleister für Akkreditierungen in Deutschland. Gesellschafter sind die Bundesrepublik Deutschland, die Bundesländer Bayern, Hamburg und Nordrhein-Westfalen sowie der Bundesverband der Deutschen Industrie e. V. (BDI) (vgl. DAkkS (o. J.-a)).

Die Akkreditierung durch die DAkkS als unabhängige Einrichtung umfasst die Begutachtung, die Bestätigung und die Überwachung der fachlichen Kompetenz der KBS. Bei den akkreditierten Stellen kann es sich um kleine bis mittlere Unternehmen sowie um multinationale Konzerne handeln. Die Akkreditierung bestätigt, dass diese Unternehmen ihre Aufgaben fachkundig und nach den geltenden Anforderungen erfüllen. Dadurch, dass die Akkreditierung von KBS als hoheitliche Aufgabe vergeben ist, soll es für Hersteller, Verbraucher und KBS ein transparentes und unabhängiges System geben. Damit trägt die DAkkS einen wichtigen Beitrag für die Qualitätssicherung von Produkten und Dienstleistungen, den Verbraucherschutz und die Wettbewerbsfähigkeit in Deutschland bei (vgl. DAkkS (o. J.-b)).

Da kein gesetzlicher Zwang für eine Akkreditierung von Zertifizierungsstellen vorhanden ist, gibt es Stellen, die akkreditiert sind und welche die nicht akkreditiert sind. Laut der DAkkS Datenbank sind 207 Zertifizierungsstellen in Deutschland zur Zertifizierung von Managementsystemen akkreditiert. Durch eine solche Akkreditierung kann sich die Zertifizierungsstelle merklich von Wettbewerbern ohne Akkreditierung abheben. Letztlich ist die Motivation eine solche Akkreditierung durchzuführen, dieselbe, wie bei Organisationen, die die Dienstleistung der Zertifizierungsstelle in Anspruch nehmen.

11.3 Zertifizierung von Risikomanagementsystemen und -prozessen

Risikomanagementsysteme sind ein wichtiger Bestandteil des Managementsystems eines Unternehmens. Das Risikomanagement versteht sich als Bindeglied zu anderen Teilbereichen des Managementsystems, wie dem Qualitäts- oder auch dem Umweltmanagement. Umso wichtiger für ein funktionierendes Risikomanagementsystem ist die Einhaltung bestimmter Standards, Normen und Richtlinien.

In diesem Abschnitt werden die Grundlagen für eine Zertifizierung näher beleuchtet. Im Anschluss wird der Ablauf einer solchen Zertifizierung aufgegriffen. Zum Schluss wird die Wirksamkeitsüberwachung von Risikomanagementsystemen durch die *IDW Prüfungsstandards* weiter ausgeführt.

11.3.1 Grundlagen

Erste Anforderungen an das Risikomanagement einer Institution werden bereits in der *DIN EN ISO 9001* (Qualitätsmanagementsysteme – Anforderungen) genannt. Dort findet vor allem der risikobasierte Ansatz Beachtung. Als Grundlage für die Zertifizierung von Risikomanagementsystemen gelten jedoch die *DIN ISO 31000* (Risikomanagement – Leitlinien) und die *ONR 49001* (Risikomanagement für Organisationen und Systeme – Risikomanagement – Umsetzung von ISO 31000 in die Praxis).

Wobei die *DIN ISO 31000* lediglich Leitlinien beschreibt, nach denen jedoch nicht zertifiziert werden kann. Für die Zertifizierung wird die österreichische Norm *ONR 49001* genutzt. Da die Inhalte für die Zertifizierung hauptsächlich in der *DIN ISO 31000* genannt sind, wird die *ONR 49001* hier nicht näher beleuchtet.

11.3.1.1 DIN EN ISO 9001 – Qualitätsmanagementsysteme Anforderungen

Die *DIN ISO 9001* beschäftigt sich mit den Anforderungen an das Qualitätsmanagement (QM) einer Organisation. Die Einführung eines QM-Systems ist eine strategische Entscheidung und soll dabei helfen, die Gesamtleistung zu steigern und für eine nachhaltige Entwicklung der Organisation sorgen. Der größte Vorteil ist vor allem die Fähigkeit, Produkte und Dienstleistungen zu liefern, die Kundenanforderungen sowie gesetzliche und behördliche Anforderungen erfüllen. Zudem können neue Chancen zur Erhöhung der Kundenzufriedenheit eröffnet werden. Darüber hinaus sollen Risiken und Chancen angemessen im Zusammenhang mit dem Kontext und den Zielen behandelt werden.

Die daraus resultierenden Grundsätze des QM sind vor allem Kundenorientierung, Führung, die Einbeziehung von Personen, ein prozessorientierter Ansatz, Verbesserung, faktengestützte Entscheidungsfindung und Beziehungsmanagement. Damit gehen folgende Ziele einher: Die Erfüllung von Produktanforderungen (gesetzliche oder von Kun-

den) und die damit verbundene Erhöhung der Kundenzufriedenheit. Zur Erreichung dieser Ziele ist es wichtig Risiken zu erfassen und zu behandeln. Dafür müssen in der Organisation verschiedene Maßnahmen eingesetzt werden. Damit werden unerwünschte Auswirkungen verhindert oder verringert. Idealerweise werden sogar Verbesserungen erreicht. Die Maßnahmen müssen im QM-Prozess und die Organisation integriert und umgesetzt werden. In der *DIN EN ISO 9001* werden diese Maßnahmen jedoch nicht weiter konkretisiert. Von hoher Relevanz ist zudem die Wirksamkeit der Maßnahmen. Daher werden diese stetig überwacht (vgl. DIN Deutsches Institut für Normung e. V. 2015, S. 8 ff.).

Die Maßnahmen werden im QM durch den Ansatz des risikobasierten Denkens verfolgt. Dies soll auf Grund der Wichtigkeit durch die oberste Leitung gefördert werden. Im QM sollen Faktoren bestimmt werden, die bewirken können, dass Prozesse und das QM-System von den geplanten Ergebnissen abweichen. Zudem sollen vorbeugende Maßnahmen zur Steuerung umgesetzt werden, um negative Auswirkungen zu minimieren und den maximalen Nutzen aus den Möglichkeiten zu ziehen. Mit der Planung und Umsetzung von Maßnahmen zur Behandlung von Risiken und Chancen wird die Wirksamkeit des QM gesteigert, es werden bessere Ergebnisse erzielt und negative Auswirkungen vermieden. Insgesamt wird das QM-System als vorbeugendes Instrument gesehen (vgl. DIN Deutsches Institut für Normung e. V. 2015, S. 53 ff.).

11.3.1.2 DIN ISO 31000 – Risikomanagement Leitlinien

Die *DIN ISO 31000* legt die Leitlinien für den Umgang mit jeglichen Risiken fest, denen Organisationen ausgesetzt sein können. In dieser Leitlinie sind die verschiedenen Begrifflichkeiten, wie zum Beispiel Risiko oder Risikomanagement (RM) sehr allgemein definiert. Daher kann diese Leitlinie auch branchenunabhängig angewendet werden.

Unter dem Begriff Risiko wird die Auswirkung von Untersicherheiten auf Ziele verstanden. Eine Auswirkung beschreibt eine positive und/oder negative Abweichung (Möglichkeiten bzw. Bedrohungen) vom Erwarteten.

Das Risikomanagement wird als „koordinierte Aktivitäten zur Lenkung und Steuerung einer Organisation in Bezug auf Risiken“ beschrieben (vgl. DIN Deutsches Institut für Normung e. V. 2018c, S. 7).

In dieser Leitlinie wird der Umgang mit Risiken als iterativ bezeichnet. Anhand des Risikomanagements können Strategien festgelegt werden, Ziele erreicht werden und Entscheidungen getroffen werden. Das Risikomanagement ist Teil aller Aktivitäten und Strukturen der Organisation.

Im Wesentlichen umfasst der Umgang mit Risiken die in Abb. 11.2 dargestellten drei Komponenten.

Die Grundsätze des RM bilden die Grundlagen für den Umgang mit Risiken. Daher sollen die Grundsätze bei der Entwicklung des Rahmenwerks und der Prozesse berücksichtigt werden. Das RM ist als strukturierter und umfassender Ansatz in alle Aktivitäten der Organisation zu integrieren. Dabei ist es so aufzubauen, dass es sich an schnell wandelnde Risiken und auch an die sich verändernde Organisation als solche dynamisch anpassen kann. Für eine wirksame Funktionsweise müssen alle historischen und aktuellen

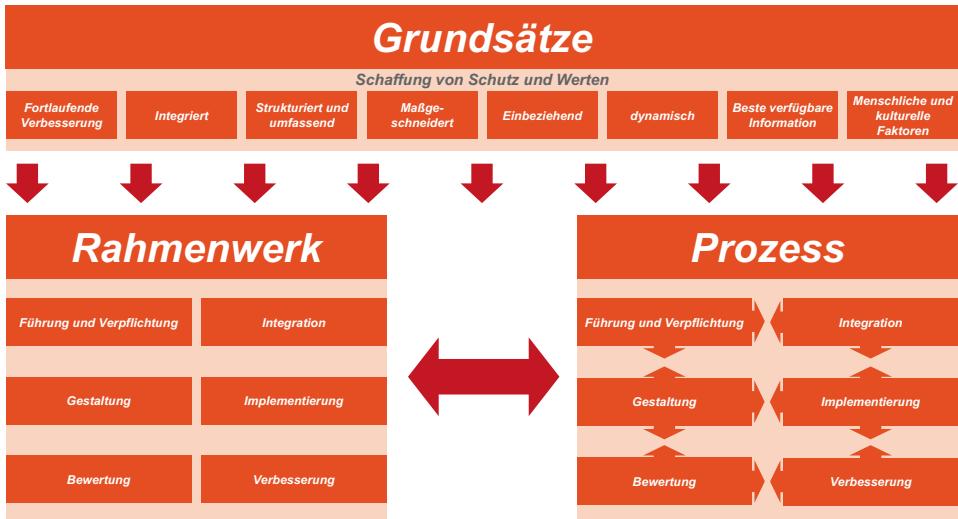


Abb. 11.2 Komponenten des Risikomanagements. (Quelle: eigene Darstellung)

Informationen sowie zukünftige Erwartungen in das RM-System mit einfließen. Hierbei sollen auch die internen und externen Stakeholder berücksichtigt werden. Weitere wichtige Punkte sind die menschlichen und kulturellen Faktoren, da diese einen wesentlichen Einfluss auf das RM haben. Letztlich müssen das Rahmenwerk und die Prozesse individuell an die Bedürfnisse und Ziele der Organisation angepasst sein (vgl. DIN Deutsches Institut für Normung e. V. 2018c, S. 9 f.).

Mithilfe des Rahmenwerks soll das RM in die bedeutenden Aktivitäten und Funktionen der Organisation integriert werden. Eine wichtige Rolle im Hinblick auf die Wirksamkeit spielt die Integration in die oberste Leitung der Organisation (Geschäftsführung bzw. Vorstand). Das RM sollte einen hohen Stellenwert in der Leitung der Organisation einnehmen. Je nach gesetzlichen Vorgaben ist das RM auch in das Aufsichtsorgan, wie zum Beispiel einen Aufsichtsrat, zu integrieren. Das Rahmenwerk ist individuell an die Bedürfnisse und Ausrichtungen der Organisation anzupassen. Die Komponenten des Rahmenwerks sind folgende (vgl. DIN Deutsches Institut für Normung e. V. 2018c, S. 11 ff.):

- **Führung und Verpflichtung:** Der Kern des Rahmenwerks ist die Führung und Verpflichtung. Die Leitung der Organisation ist für den Umgang mit Risiken verantwortlich. Daher ist sicherzustellen, dass alle Komponenten des Rahmenwerks umgesetzt werden. Dafür muss gewährleistet sein, dass ausreichend Ressourcen zur Verfügung gestellt werden. Damit geht einher, dass die Teile der Organisation, die sich explizit mit dem RM beschäftigen, die erforderlichen Befugnisse und Verantwortlichkeiten erhalten. Somit wird garantiert, dass das RM-Rahmenwerk den Anforderungen der Ziele, Strategie und Kultur der Organisation gerecht wird. Diese und weitere Ansätze und Maßnahmen im Rahmen des RM sollen (zum Beispiel in einem Dokument) in der Or-

ganisation veröffentlicht werden. Somit sind alle internen Stakeholder im Hinblick auf die Risikosteuerung, -entwicklung und -überwachung und deren Wert ausreichend informiert. Neben der Leitung der Organisation ist auch das Aufsichtsorgan einer Organisation vor allem für die Überwachung der RM-Systeme zuständig. Daher ist das Aufsichtsorgan dazu angehalten bei Strategie- und Zielfestlegung, Risiken zu berücksichtigen, zu verstehen und die Angemessenheit zu beurteilen. Für den Umgang solcher Risiken muss das Aufsichtsorgan sicherstellen, dass ein entsprechendes System in der Organisation integriert wird.

- **Integration:** Da das RM Bestandteil aller Aktivitäten und Strukturen einer Organisation ist, müssen die Strukturen und deren Zielen, Zwecke und Komplexität verstanden werden. Letztlich ist jeder in der Organisation für den Umgang von Risiken mitverantwortlich. Daher sollte das RM Teil der Führung, der Strategie, der Ziele und der Abläufe sein. Diese Integration ist ein dynamischer und iterativer Prozess, der an die Bedürfnisse und Kultur der Organisation anzupassen ist.
- **Gestaltung:** Für die Gestaltung des Rahmenwerks ist es unerlässlich, dass die Organisation verstanden wird. Dabei sind der interne (unter anderem Vision, Mission, Leistung, Struktur, Strategie, Ziele, Kultur, Fähigkeiten) und der externe (zum Beispiel finanzielle oder politische Faktoren, Trends, Beziehungen, Netzwerke) Kontext der Organisation von hoher Relevanz. Zudem ist das Bewusstsein zu einer dauerhaften Verpflichtung zum Risikomanagement ein weiterer wichtiger Punkt. Die Leitung muss dies nachweisen und gegenüber der Organisation und ggf. weiteren Stakeholdern kommunizieren. Dies kann, wie weiter oben bereits genannt, zum Beispiel mit einem Dokument geschehen, in dem unter anderem die Gründe für das RM, die Notwendigkeit, Integration, Verantwortlichkeiten, vorhandenen Ressourcen und die Berichterstattung erläutert sind. Die Leitung hat sicherzustellen, dass alle relevanten Rollen und die damit einhergehenden Verantwortlichkeiten, Befugnisse und Rechenschaftspflichten vergeben und kommuniziert sind. Neben der Rollenverteilung spielt die Zuordnung von Ressourcen eine bedeutende Rolle. Dazu können zum Beispiel Personen, Fähigkeiten, Prozesse, Methoden, Systeme und Weiterentwicklungsmöglichkeiten gehören. Zur Unterstützung des Rahmenwerks ist eine Kommunikations- und Konsultationsstelle einzurichten. So kann sich einfacher ausgetauscht werden und Feedback eingeholt werden.
- **Implementierung:** Die Implementierung des Rahmenwerks sollte durch einen geeigneten Plan vorgenommen werden, der festlegt, wie der Entscheidungsfindungsprozess aussieht und die Vorbereitungen verstanden und angewendet werden. Für eine erfolgreiche Implementierung ist Engagement und Bewusstsein der internen und externen Stakeholder von Nöten. So wird das RM Teil aller Aktivitäten und Entscheidungsfindungen und kann sich angemessen an Änderungen des internen und externen Kontextes anpassen.
- **Bewertung:** Für eine Bewertung der Wirksamkeit des Rahmenwerks muss die Organisation die Leistung des RM-Rahmenwerks stetig im Hinblick auf die Anforderungen überprüfen. Dabei wird hinterfragt, ob es noch immer geeignet ist, um die Ziele der Organisation zu erreichen.

- **Verbesserung:** Neben der Bewertung ist die Verbesserung ein wichtiger Bestandteil. Dabei steht die kontinuierliche Überprüfung und entsprechende Anpassung an interne und externe Veränderungen im Fokus. Sobald relevante Lücken in der Eignung, Angemessenheit oder Wirksamkeit erkannt werden, sollen diese geschlossen und weitere Verbesserungsmöglichkeiten genutzt werden.

Mit dem RM-Rahmenwerk geht der iterative RM-Prozess einher. Dieser umfasst die Anwendung der Grundsätze, Verfahren und Prozesse auf die Kommunikation und Konsultation, den Kontext, die Beurteilung, die Behandlung, das Überwachen und Überprüfen sowie das Aufzeichnen und Berichten.

Der RM-Prozess ist integraler Bestandteil des Managements und der Entscheidungsfindung und muss in alle Strukturen, Abläufe und Aktivitäten der Organisation integriert sein. Wichtig ist, dass im Prozess das menschliche Verhalten und die Kultur berücksichtigt werden.

- **Kommunikation und Konsultation:** Wie bei allen Prozessen in einer Organisation spielt die Kommunikation eine tragende Rolle. Die Stakeholder können die Beweggründe für gewisse Aktivitäten besser verstehen. Somit wird das Risikobewusstsein und -verständnis gefördert. Die Konsultation ist ein wichtiges Mittel zum Einholen von Feedback. So können verschiedene Stakeholder ihre Fachkenntnisse, ihre Ansichten und ihre Informationen einbringen, um eine bessere Bewertung, Überwachung und Behandlung der Risiken vornehmen zu können. Die Kommunikation und Konsultation sollte in allen Schritten des RM-Prozesses stattfinden.
- **Anwendungsbereich, Kontext und Kriterien:** Bei der Bestimmung des Anwendungsbereichs, den Kontexten und der Kriterien geht es darum, einen maßgeschneiderten RM-Prozess mit einer wirksamen Risikobeurteilung und einer geeigneten Risikobehandlung zu ermöglichen. Hierbei werden der Anwendungsbereich des Prozesses, ein Verständnis des internen und externen Kontextes und Kriterien zur Beurteilung der Signifikanz von Kriterien geschaffen. Für die Festlegung des geeigneten Anwendungsbereichs müssen vor allem die Ziele, die Anpassungen und die einzelnen Bereiche verstanden werden. Daher sind bei der Festlegung verschiedenste Faktoren, wie Entscheidungen, Ergebnisse, Zeitpunkt, Verfahren zur Risikobeurteilung, Ressourcen und Verantwortlichkeiten zu berücksichtigen. Als Kontext wird das interne und externe Umfeld verstanden, in dem die Organisation agiert. Das RM einer Organisation sollte an deren Ziele, Aktivitäten und Faktoren angepasst sein. Diese Punkte drücken sich weitestgehend im Umfeld/Kontext aus. Da auf dieses Umfeld der Risikomanagementprozess angewendet wird, ist ein Verständnis des Kontextes von hoher Relevanz. Die Risikokriterien sollen das Maß der Signifikanz der einzelnen Risiken wiedergeben und den Entscheidungsfindungsprozess unterstützen. Diese sind genauestens auf das RM-Rahmenwerk abzustimmen, an die Aktivitäten angepasst und im Einklang mit den Grundsätzen des RM. Die Risikokriterien sind zu Beginn des Beurteilungsprozesses festzulegen und ständig dynamisch zu überprüfen und Bedarfsfall zu ändern. Bei der

Festlegung sollten unterschiedliche Faktoren berücksichtigt werden: Natur und Art der Unsicherheiten, Festlegung und Messung der Auswirkungen und Wahrscheinlichkeiten des Eintritts, zeitliche Faktoren, Bestimmung der Risikohöhe, Berücksichtigung des Eintritts mehrerer Risiken hintereinander, Kapazität der Organisation.

- **Risikobeurteilung:** Die Beurteilung umfasst den Prozess der Risikoidentifikation, -analyse und -bewertung. Auch dieser Prozess verläuft systematisch, iterativ und kollaborativ unter Nutzung der (Fach-)Kenntnisse der Stakeholder. Im Rahmen der Risikoidentifikation werden Risiken erkannt und beschrieben. Dabei werden alle relevanten, geeigneten und aktuellen Informationen genutzt. Nach der Identifizierung von Risiken erfolgt die Analyse dieser. Dabei soll die Art, die Eigenschaft und die Höhe des Risikos verstanden werden. Bei der Analyse werden verschiedene Faktoren betrachtet, unter anderem Wahrscheinlichkeiten, Auswirkungen und Wirksamkeit von Steuerungselementen. Eine Analyse kann unterschiedlich detailreich oder komplex durchgeführt werden. Prinzipiell wird zwischen quantitativen und/oder qualitativen Analysen unterschieden. Für den Fall, dass zum Beispiel sehr ungewisse Ereignisse eintreten, empfiehlt sich die Durchführung einer Kombination von quantitativen und qualitativen Analysen. Die Analyse liefert einen wichtigen Beitrag für die Risikobewertung und -behandlung. Die Risikobewertung nutzt die Ergebnisse der Analyse, um diese mit den festgelegten Risikokriterien zu vergleichen und Entscheidungen zu unterstützen. Beispiele für diese Entscheidungen können sein, dass nichts weiter unternommen wird, weitere Analysen für ein besseres Risikoverständnis durchgeführt werden, das Risiko „behandelt“ wird oder die bestehenden Ziele überdacht werden. Bei der Entscheidungsfindung sollte jedoch immer der breite Kontext und die Auswirkungen berücksichtigt werden.
- **Risikobehandlung:** Bei der Risikobehandlung werden Optionen zur Behandlung des Risikos ausgewählt und implementiert. Wichtig ist, dass es sich hierbei wiederum um einen iterativen Prozess handelt, der stets wiederholt wird. Erst werden Maßnahmen zur Risikobehandlung ausgewählt. Dabei wird, wie bei jeder Entscheidung zwischen Vorteilen und Nachteilen abgewogen. Solche Maßnahmen können unter anderem sein, dass die Aktivität, die das Risiko verursacht, eingestellt wird oder das Risiko erhöht wird, um eine Chance zu nutzen. Bei der Entscheidungsfindung sollten neben den wirtschaftlichen Faktoren bedacht werden, dass die Maßnahme im Einklang mit den Zielen/Strategien steht, die Maßnahme kommuniziert werden muss, Überwachungen und Überprüfungen vorgenommen werden müssen und die Maßnahme zu neuen Risiken führen kann oder ein Restrisiko bestehen bleibt. Nach der Wahl der Maßnahme zur Risikobehandlung folgt nun die Erstellung von Plänen zur Implementierung der Maßnahme.
- **Überwachen und Überprüfen:** Das Überwachen und Überprüfen befasst sich mit der Sicherstellung und Verbesserung der Qualität und Wirksamkeit der Planung, Implementierung und Ergebnisse des Prozesses. Dieser Teil sollte in allen Phasen des RM-Prozesses stattfinden und mit einer festen Verantwortlichkeit versehen sein. Die Ergebnisse sind im Berichtswesen der gesamten Organisation mit eingebunden.
- **Aufzeichnen und Berichten:** Der RM-Prozess und seine Ergebnisse sollen dokumentiert und kommuniziert werden. Die Aktivitäten und Ergebnisse können so der gesamten

Organisation zur Verfügung gestellt werden. Das Berichten ist integraler Bestandteil der Leitung der Organisation und zur Unterstützung bei der Erfüllung der Verpflichtungen beitragen (vgl DIN Deutsches Institut für Normung e. V. 2018c, S. 16 ff.).

Auf Grund der neutralen Formulierungen wie zum Beispiel „angemessen“, „individuell“ oder auch „angepasst“ sind die Leitlinien der *DIN ISO 31000* auf die verschiedensten Branchen und Unternehmen anwendbar. Anhand dieser Leitlinien kann jedes Unternehmen/jede Organisation unabhängig der Größe ein wirksames RM-System einrichten. Eine Zertifizierung nach diesen Leitlinien ist aus auf Grund der neutralen und auch teilweisen unkonkreten Formulierungen jedoch nicht möglich. Für die Zertifizierung wird die österreichische Norm *ONR 49001* genutzt, die die Leitlinien der *DIN ISO 31000* in konkrete Anforderungen an das Risikomanagementsystem formuliert. Neben der *ONR 49001* gibt es noch die *ONR 49002* (Leitfaden für verschiedene Teile des RM) und die *ONR 49003* (Anforderungen an den Risikomanager).

11.3.2 Ablauf einer Zertifizierung

Bei einer Zertifizierung handelt es sich, wie bereits erläutert, um eine besondere Form des Audits. Diese Form des Drittparteien-Audits wird durch eine externe, ggf. akkreditierte sogenannte Konformitätsbewertungsstelle/Zertifizierungsstelle durchgeführt. Diese Zertifizierungsstelle muss unparteilich, vertraulich, offen, verantwortungsvoll und kompetent sein (vgl. DIN Deutsches Institut für Normung e. V. 2015, S. 13 ff.).

Das Programm eines Zertifizierungsaudits ist teilweise durch die *DIN EN ISO/IEC 17021-1* geregelt. Zu Beginn wird ein Vertrag mit der Zertifizierungsstelle, die den o. g. Anforderungen der *DIN EN ISO/IEC 17021-1* nachkommt, geschlossen. Anschließend wird das Audit in zwei Stufen durchgeführt. Es folgt der Auditbericht, die Zertifikatserteilung und die Durchführung von Folgemaßnahmen. Im Gegensatz zu anderen Zertifizierungen werden weitere Überwachungsaudits und nach drei Jahren eine Rezertifizierung durchgeführt. Daher werden die Verträge mit Zertifizierungsstellen häufig für eine Dauer von mind. drei Jahren geschlossen.

In der Vorbereitungsphase wird der Vertrag mit der Zertifizierungsstelle geschlossen. Dabei werden erste Informationen ausgetauscht und die Anforderungen an die zu zertifizierende Organisation werden gestellt.

In der Audit Stufe 1 wird eine Kernfrageliste, in der der Auditor Kennzeichen des Risikomanagementsystems abfragt, erstellt. Die Frageliste orientiert sich an den Leitlinien der ISO 31000 und der ONR 49001. Hiermit soll der aktuelle Stand des Risikomanagementsystems und der dazugehörigen Prozesse ermittelt werden.

Die Audit Stufe 2 befasst sich mit der Sammlung von Auditnachweisen. Damit soll die Zertifizierungsfähigkeit der Organisation festgestellt bzw. bewertet werden. Das Resultat aus den Auditnachweisen führt zu Auditfeststellungen. Je nachdem, wie die zu zertifizierende Organisation die Anforderungen erfüllt, wird eine Schlussfolgerung getroffen. Wenn

zu viele und kritische Abweichungen auffallen, kann die Zertifizierung versagt oder auch abgebrochen werden. Bei geringen Nebenabweichungen kann die Zertifizierung mit Auflagen empfohlen werden. Wenn genügend Konformitäten gegeben sind, wird die Zertifizierung ohne Auflagen oder Einschränkungen empfohlen. Für den Fall, dass die Empfehlung ausgesprochen wird, wird das Zertifizierungsdokument mit den Inhalten gemäß DIN EN ISO/IEC 17021 erstellt.

Neben dem Zertifizierungsdokument wird ein Bericht erstellt. Dieses enthält vor allem folgende Punkte:

- Anmerkungen zu Konformitäten, Nichtkonformitäten, Korrekturen und Maßnahmen;
- Bestätigung der gelieferten Informationen;
- Empfehlung über Gewährung/Nicht-Gewährung der Zertifizierung inkl. Bedingungen/Beobachtungen.

Der Bericht wird von der Zertifizierungsorganisation auf Plausibilität geprüft.

Im Anschluss an die eigentliche Zertifizierung werden jährliche Überwachungsaudits durchgeführt. Mit diesen Überwachungsaudits wird die Wirksamkeit des Risikomanagementsystems überwacht. Dieses Vor-Ort-Audit hat nicht den gleichen Umfang wie ein Zertifizierungsaudit. Es fokussiert sich unter anderem auf die Schwerpunkte interne Audits, Managementbewertung, Abstellung von Nichtkonformitäten, und Behandlung von Beschwerden etc. Neben den Überwachungsaudits wird nach drei Jahren eine Rezertifizierung vorgenommen. Diese Rezertifizierung hat bis auf die Audit Stufe 1 den gleichen Umfang wie die vorherige Zertifizierung. Die Audit Stufe 1 wird nur bei signifikanten Änderungen des Managementsystems durchgeführt (vgl. Brauweiler et al. 2015, S. 27 ff.)

Neben der Rezertifizierung kann die Wirksamkeit des Risikomanagementsystems ebenfalls durch einen Wirtschaftsprüfer geprüft werden.

11.3.3 Überprüfung von Risikomanagementsystemen durch den Wirtschaftsprüfer

Funktionierende Risikomanagementsysteme spielen in allen Arten von Organisationen eine tragende Rolle. In Aktiengesellschaften fällt durch das duale Führungssystem die Verantwortung für ein funktionierendes RM-System dem Aufsichtsrat (Aufsichtsorgan) und dem Vorstand (Leitung der Organisation) zu. Der Vorstand leitet das Unternehmen, während der Aufsichtsrat die Geschäftsführung/den Vorstand überwacht.

Im Deutschen Corporate Governance Kodex ist geregelt, dass der Vorstand für ein angemessenes Risikomanagement zu sorgen hat. Der Aufsichtsrat hingegen ist, zum Beispiel in Form eines Prüfungsausschusses, für die Überwachung der Wirksamkeit des Risikomanagementsystems zuständig (§ 107 Abs. 3 AktG). Die gesetzliche Überwachungsfunktion des Aufsichtsrats kann nicht durch andere wahrgenommen werden.

Eine Zertifizierung des RM-Systems kann eine Grundlage für die Überwachungsarbeit bilden. Darüber hinaus besteht die Möglichkeit, einzelne oder mehrere Corporate Governance Systeme (unter anderem das RM-System) durch einen Wirtschaftsprüfer überprüfen zu lassen. Diese Überprüfung kann als Grundlage für die eigene Beurteilung dienen, um der aus dem § 111 Abs. 1 AktG resultierenden Pflicht der Überwachung nachkommen zu können. Auch der Vorstand partizipiert an einem objektiven Nachweis durch den Wirtschaftsprüfer, da so nachgewiesen werden kann, dass er der fehlerfreien Ausübung der Organisations- und Sorgfaltspflicht nachgekommen ist.

Zielsetzung der Systemprüfung ist die Beurteilung, inwieweit das Unternehmen durch Einrichtung eines RM-Systems, Risiken, die den festgelegten Zielen des RM-Systems entgegenstehen, rechtzeitig identifiziert, bewertet, steuert und überwacht (vgl. IDW PS 981, Tz. 8.).

Gegenstand einer solchen Prüfung ist die RM-Systembeschreibung. In dieser sind die Regelungen und Grundsätze des RM-Systems beschrieben.

Ziel der Wirksamkeitsprüfung ist es, zu überprüfen, ob die im geprüften Zeitraum implementierten Regelungen in der RM-Systembeschreibung in Übereinstimmung mit den angewandten Grundsätzen angemessen dargestellt sind. Zudem wird geprüft, ob die genannten Regelungen während des geprüften Zeitraums geeignet waren, die wesentlichen Risiken, rechtzeitig zu erkennen, zu bewerten, zu steuern und zu überwachen. Letztlich wird analysiert, wie wirksam die Regelungen waren. Die Wirksamkeit ist dann gegeben, wenn die Regelungen in den laufenden Geschäftsprozessen von den jeweils Betroffenen in einem bestimmten Zeitraum wie geplant eingehalten werden.

Neben der Wirksamkeitsprüfung ist die Durchführung einer Angemessenheitsprüfung möglich. In jeder Wirksamkeitsprüfung wird ebenfalls eine Angemessenheitsprüfung durchgeführt. Mit einer solchen Prüfung wird untersucht, ob die im geprüften Zeitraum implementierten Regelungen in der RM-Systembeschreibung in Übereinstimmung mit den angewandten Grundsätzen angemessen dargestellt sind und ob die genannten Regelungen während des geprüften Zeitraums geeignet waren, die wesentlichen Risiken, rechtzeitig zu erkennen, zu bewerten, zu steuern und zu überwachen. Jedoch wird hier nicht die Wirksamkeit überprüft, sondern, ob die Regelungen vollumfänglich implementiert waren. Eine Angemessenheit ist dann gewährleistet, wenn die Regelungen implementiert sind und geeignet sind, die wesentlichen Risiken, die dem Erreichen der Ziele des RM-Systems entgegenstehen, rechtzeitig zu erkennen, zu bewerten, zu steuern und zu überwachen. Ebenfalls muss die Überwachung der RM-Systeme hinsichtlich Eignung zur Umsetzung der Risikostrategie und Erreichung der Ziele des RM-Systems.

Auf diese Art und Weise können nicht nur bestehende RM-Systeme geprüft werden. Unternehmen, die ein solches Corporate Governance System erstmalig einführen oder erweitern, können eine Angemessenheitsprüfung während allen Projektphasen durch den Wirtschaftsprüfer durchführen lassen (vgl. PS 981, Tz. 21ff).

11.4 Zertifizierter Risikomanager

Neben einer Zertifizierung der Risikomanagementsysteme besteht auch die Möglichkeit, dass sich Personen, die viele Berührungspunkte mit dem RM-System haben, als Risikomanager zertifizieren lassen. Dafür hat der europäische Risikomanagement-Verband, *Federation of European Risk Management Associations (FERMA)*, ein Zertifizierungsprogramm für Risikomanager herausgebracht. Dieses setzt einen Standard für die Qualifikation von Risikomanagern in Europa. Neben Fachwissen und Berufserfahrung fließen ebenfalls das Einhalten von Ethik-Grundsätzen und Standards in die Bewertung ein.

Die *Rimap Certification* wurde Anfang 2016 vom europäischen Verband *FERMA* veröffentlicht. Ziel der *FERMA* und der tragenden nationalen Verbände war es, einheitliche und europaweite Qualifizierungs-Standards für Risikomanager zu schaffen, die bis dahin noch nicht existierten.

Die Zertifizierung richtet sich an Mitarbeiter im Bereich des Risiko- und Insurancemanagements. Voraussetzung für die Teilnahme ist eine gewisse Berufserfahrung. Die Anzahl an Jahren hängt von der Qualifikation des Bewerbers ab (zum Beispiel Bachelor- oder Masterabschluss).

Es werden zwei verschiedene Zertifizierungslevels angeboten. Das sind das *Rimap Level* und das *Rimap Advanced Level*. Das *Rimap Advanced Level* behandelt weitestgehend die gleichen Themen, wie das *Rimap Level*, vertieft diese aber noch weiter. Zudem sind ein bereits vorhandenes tiefergehendes Fachwissen und eine längere Berufserfahrung erforderlich, um die *rimap advanced Level* Zertifizierung zu absolvieren. Daher ist das *Rimap Level* eher für Berufsanfänger und das *Rimap Advanced Level* für Berufserfahrenre gedacht.

Zur Aufrechterhaltung der Zertifizierung müssen sogenannte *Continuous Professional Development (CPD) points* gesammelt werden. Diese Weiterbildungspunkte können durch Seminare, Veranstaltungen oder auch durch Veröffentlichungen und Interviews gesammelt werden (vgl. Speyrer 2016, S. 1).

Die Zertifizierung befasst sich mit mehreren Themenblöcken. Wobei die letzten beiden Themen eher für das *Rimap Advanced Level* relevant sind.

- **Grundlagen des Risikomanagements:** Zu Beginn wird das vier Säulen Modell der *rimap certification* aufgezeigt (Wissen, Erfahrung, Einhalten von Ethik-Grundsätzen, regelmäßige Weiterbildung). Darüber hinaus wird Basiswissen rund um das (betriebliche) Risikomanagement erwartet.
- **Risikobewertung:** Dieser Themenblock umfasst den Prozess der Risikoidentifikation, -bewertung und -evaluation innerhalb einer Organisation. Dabei werden unterschiedliche Klassifizierungen, Techniken, Analyse Tools und Modelle behandelt.
- **Riskobehandlung I:** Aufbauend auf der Bewertung werden in diesem Abschnitt Mechanismen und Tools zur Behandlung von Risiken und Schäden dargelegt. Der Schwerpunkt liegt auf Kontrolle und Reduzierung der Risiken und der möglichen Schäden.

- **Risikobehandlung II:** Dieser Block umfasst Finanzmaßnahmen zur Risikobehandlung. Vor allem wird das Thema (Rück-)Versicherung vertieft.
- **Kommunikation und Überwachung:** Dieser Abschnitt ist größtenteils nur für das *rimap advanced Level* relevant. Hier werden Themen wie Kommunikation und Konsultation mit Stakeholdern, Überwachungssysteme und Reportings behandelt.
- **Besondere Risikomanagement Themen:** Im letzten Themenblock werden bestimmte Unternehmensbereiche im Rahmen des Risikomanagements beleuchtet. Dies sind unter anderem operationelle Risiken, Lieferketten-Risiken, Krisenmanagement und Betriebsunterbrechungsmanagement. Dieser Abschnitt ist vollständig nur für das *rimap advanced Level* relevant (vgl. Federation of European Risk Management Associations 2015, S. 7 ff.).

Die Vorteile einer *Rimap Certification* sind aus mehreren Perspektiven zu betrachten. Die zertifizierte Person kann sich klar von Mitbewerben auf dem Stellenmarkt differenzieren und somit die persönlichen Karrierechancen auch auf internationalem Umfeld steigern.

Auch Organisationen haben Vorteile dadurch, dass ihre Mitarbeiter im RM-Bereich zertifiziert sind. Damit kann gezeigt werden, dass das RM innerhalb der Organisation ernst genommen wird, da kompetente und zertifizierte Mitarbeiter sich mit diesem Thema befassen. Darüber hinaus kann die Reputation und die Glaubwürdigkeit gegenüber den Stakeholdern gesteigert werden.

11.5 Fazit

In Zeiten zunehmender Globalisierung, dynamischer werdender Umfelder und immer weiter voranschreitender Digitalisierung nimmt die Anzahl an Risiken innerhalb einer Organisation immer weiter zu. Heutzutage sind vor allem Marktrisiken, wie zum Beispiel ein wirtschaftlicher Rückgang oder sich schnell verändernde Marktfaktoren, und Cyber-Risiken von großer Relevanz. Umso wichtiger werden daher der Umgang und die Behandlung eben solcher Risiken im Rahmen des betrieblichen Risikomanagements.

Das Risikomanagement spielt im globalen Managementsystem einer Organisation eine tragende Rolle. Es kann als Bindeglied zu anderen Teilbereichen des Managementsystems, wie dem Qualitäts- oder auch dem Umweltmanagement, gesehen werden. Dies wird vor allem dadurch deutlich, dass das Risikomanagement in den Leitlinien und Normen zu den verschiedenen Managementstandards als relevanter Teil dargestellt wird, wie zum Beispiel im risikobasierten Denken der *DIN EN ISO 9001*. Die expliziten Anforderungen an das Risikomanagementsystem werden jedoch in den gesonderten Leitlinien der *DIN ISO 31000* genannt. Im Kern dieser Leitlinien steht der Umgang mit Risiken. Dieser kennzeichnet sich vor allem dadurch, dass das Risikomanagement in die oberste Leitung der Organisation integriert wird. Somit soll gewährleistet werden, dass dem Risikomanagementsystem die entsprechende Priorität innerhalb der Organisation eingeräumt wird. Die Formulierungen innerhalb der Leitlinien sind jedoch so neutral formuliert, dass die Leitli-

nien auf die verschiedensten Unternehmen jeder Größer und aus jeder Branche anwendbar sind. Da es sich jedoch hierbei nur um Leitlinien handelt, wird für die Zertifizierung die österreichische Norm *ONR 49001* genutzt.

Der Zertifizierungsprozess wird in mehrere Stufen eingeteilt. In den unterschiedlichen Audit Stufen werden aufbauend auf der *DIN ISO 31000* und der *ONR 49001* detaillierte Informationen mit Blick auf die Risikomanagementprozesse und -systeme abgefragt. Diese tief greifenden Informationen über das Unternehmen sollen der Organisation und der externen Zertifizierungsstelle die Qualität nachweisen und sicherstellen. Die dem Auditor bekannten Details über das Unternehmen können jedoch nicht nur für die Zertifizierung von Relevanz sein. Auch andere externe Parteien können von zertifizierten Risikomanagementsystemen profitieren. Am ehesten kommen dafür Versicherungsunternehmen in Frage, da diese in vielen Bereichen des Risikomanagements mitwirken. Klassisch spielen die Versicherer beim Risikotransfer eine wichtige Rolle. Wird jedoch das zu transferierende Risiko dadurch gemindert, dass Risiken durch ein funktionierendes Risikomanagementsystem besser vermieden oder verhindert werden, profitiert dadurch ebenfalls der Versicherer. Dies wird jedoch selten im Underwriting des Versicherungsunternehmens berücksichtigt.

Daher kann ein zertifiziertes Risikomanagementsystem für eine bessere und äquivalente Risikoeinschätzung genutzt werden.

Literatur

- Aon plc. (2019). *Global risk management survey 2019*. <https://www.aon.com/getmedia/6b9cacef-3ba1-4360-b470-dff66ce29d1a/aon-global-risk-management-survey-report-2019.pdf.aspx>. Zugriffen am 08.05.2019.
- Brauweiler, J., Will, M., & Zenker-Hoffmann, A. (2015). *Auditierung und Zertifizierung von Managementsystemen: Grundwissen für Praktiker*. Wiesbaden: Springer Gabler.
- DAkkS. (o. J.-a). *Aufgaben*. <https://www.dakks.de/content/welche-aufgabe-hat-die-dakks>. Zugegriffen am 27.01.2020.
- DAkkS. (o. J.-b). *Profil*. <https://www.dakks.de/content/profil>. Zugegriffen am 27.01.2020
- DIN Deutsches Institut für Normung e. V. (2015). *Konformitätsbewertung – Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren – Teil 1: Anforderungen (ISO/IEC 17021-1:2015): Deutsche und Englische Fassung EN ISO/IEC 17021-1:2015*. Berlin: Beuth.
- DIN Deutsches Institut für Normung e. V. (2018a). *Konformitätsbewertung – Anforderungen an Akkreditierungsstellen, die Konformitätsbewertungsstellen akkreditieren (ISO/IEC 17011:2017): Deutsche und Englische Fassung EN ISO/IEC 17011:2017*. Berlin: Beuth.
- DIN Deutsches Institut für Normung e. V. (2018b). *Leitfaden zur Auditierung von Managementsystemen (ISO 19011:2018): Deutsche und Englische Fassung EN ISO 19011:2018*. Berlin: Beuth.
- DIN Deutsches Institut für Normung e. V. (2018c). *Risikomanagement – Leitlinien (ISO 31000:2018)*. Berlin: Beuth.
- DQS GmbH. (o. J.). *Was ist eine High Level Strucuture?* <https://www.dqs.de/de/audits/die-high-level-structure-im-ueberblick/>. Zugegriffen am 27.01.2020.
- Federation of European Risk Management Associations. (2015). *rimap – Certified Risk Management Professional: Body of Knowledge September 2015*.

Friedel, R., & Spindler, E. A. (Hrsg.). (2016). *Zertifizierung als Erfolgsfaktor*. Wiesbaden: Springer Fachmedien.

International Organization for Standardization (Hrsg.). (2018). „The ISO Survey of Management System Standard: Certifications – 2017 – Explanatory Note“.

International Organization for Standardization (Hrsg.). (o. J.) „ISO Management System Standards“. Speyrer, S. 2016. Interview mit Dirk Wegener. Zugriffen am 31.05.2019.

Olaf Seiche ist in Hamburg geboren und aufgewachsen. Er studierte Produktionstechnik an der FH Hamburg. Während seiner Berufslaufbahn übernahm er von 1992 bis 2002 Consultingtätigkeiten für diverse Industrie- und Dienstleistungsbetriebe. Im Jahr 2002 trat er in die TÜV Rheinland Group ein. In seiner heutigen Position als Regional Field Manager Customized Auditing Solutions und Prokurstatist hat er die Kostenstellenverantwortung für über 60 Mitarbeiter und ca. acht Millionen Euro Umsatz. Außerdem hat er die bundesweite Geschäftsfeldverantwortung über alle Gesellschaften der TÜV Rheinland Gruppe Deutschland im Bereich der Customized Lösungen im Auditierungs- und Zertifizierungssegment. Im Einzelnen handelt es sich dabei um folgende Tätigkeitsschwerpunkte: Das globale Business Development in Ländern wie Europa, Südafrika, Dubai, Saudi Arabien, Thailand, Taiwan und Japan, die Entwicklung von Zertifizierungsstandards in den Themengebieten Qualität, Umwelt, Nachhaltigkeit, Servicequalität und Safety & Security, die Entwicklung und Einführung von QFM Systemen für Dienstleistungs- und Produktionsunternehmen, die Entwicklung und Einführung von Quality Checks, Ausbildung internationaler Auditoren (zum Beispiel Saudi Tourism Council), die Gremienarbeit in Verbänden, Marktanalysen, Standort- und Zielgruppenanalyse, Legal Compliance von der Beschaffung bis zum After-Sales, sowie die Ausbildung, Bewertung und das Monitoring von Auditoren. Herr Seiche ist zudem zugelassener Senior Auditor ISO 9001:2015. Neben seiner Tätigkeit beim TÜV Rheinland nimmt Herr Seiche auch Dozententätigkeiten in den Bereichen Medien, Marketing, Tourismusmanagement sowie Tourismusforschung an der Hochschule Darmstadt und der Fresenius Hochschule wahr.

Erik Klaedtke absolvierte ein duales Studium bei der RheinLand Versicherungsgruppe. Im Rahmen dessen schloss er sein Bachelorstudium im Fach Versicherungswesen mit den Schwerpunkten Rückversicherung, Sach- und Betriebsunterbrechungsversicherung und Versicherungsmarketing am Institut für Versicherungswesen der Technischen Hochschule Köln ab. Parallel durchlief er die Ausbildung zum Kaufmann für Versicherungen und Finanzen bei der IHK Mittlerer Niederrhein. Anschließend absolvierte er den konsekutiven Masterstudiengang Risk & Insurance. Zudem ist er weiterhin bei der Credit Life AG, ein Unternehmen innerhalb der RheinLand Versicherungsgruppe, als Key Account Manager im Banken- und Kooperationsvertrieb beschäftigt.



Corporate Governance und Compliance

12

Definition, Risiken und Haftungsfragen

Andreas Biegel und Pascal Müller

Zusammenfassung

Corporate Governance und Compliance haben in den letzten Jahrzehnten zunehmend an Bedeutung gewonnen. Grund dafür waren pressewirksame Vorfälle, die hohe Geldstrafen, Klagen und Reputationsverlust für die betroffenen Unternehmen zur Folge hatten. Die Auslöser waren vor allem Korruptions- und Geldwäsche Fälle. In jedem dieser Fälle wurde die Verantwortlichkeit der Organe und sonstiger Entscheidungsträger im Unternehmen thematisiert. Neben der Freiheit, unternehmerische Entscheidungen treffen zu können, bildet dieser Personenkreis gleichzeitig das zentrale Element eines funktionsfähigen Risikomanagement-Systems. Damit einhergehend sind die fachlichen und persönlichen Anforderungen an diesen Personenkreis immer weiter gestiegen. In diesem Zusammenhang haben auch die Themen Datenschutz und IT-Compliance aktuell Bedeutung erlangt. Durch die voranschreitende Digitalisierung entstehen stetig neue Herausforderungen für Unternehmen und die handelnden Personen. Neben der Vermeidung negativer Effekte, die durch Verstöße gegen Compliance-Bestimmungen einschließlich Corporate-Governance-Richtlinien entstehen können, gibt es auf der anderen Seite jedoch auch Vorteile, wenn ein Unternehmen die bestehenden Compliance-Anforderungen beachtet. Wie sieht allerdings der rechtliche Rahmen genau aus? Welche Personen sind im Unternehmen betroffen? Wie stellt sich die Haftungssituation für Unternehmen und deren Organe und bestimmte Mitarbeiter dar? Diese und weitere Fragen werden im Rahmen dieses Kapitels beleuchtet und analysiert.

A. Biegel (✉)

Delvag Versicherungs-AG, Köln, Deutschland

E-Mail: andreas.biegel@delvag.de

P. Müller

TH Köln, Institut für Versicherungswesen, Köln, Deutschland

E-Mail: pascal-m-92@web.de

12.1 Definitionen von Corporate Governance und Compliance

12.1.1 Corporate Governance

Corporate Governance steht für eine verantwortungsbewusste Unternehmensführung, die Risiken und gesetzliche Anforderungen im Blick hat und daher bestimmte Strukturen für ein Unternehmen vorsehen muss (vgl. Rohlfs 2019, S. 33). Das Ziel ist eine nachhaltige Wertschöpfung im Unternehmenskontext. In der US-amerikanischen Unternehmensführung spielt Corporate Governance seit langer Zeit eine übergeordnete Rolle. In Deutschland erlangte das Thema vor allem dadurch Bekanntheit, dass namhafte Unternehmen gegen die Grundsätze ordnungsgemäßer Unternehmensführung verstoßen haben. Dies hatte Geldbußen im bis zu dreistelligen Millionenbereich sowie schwerwiegende Reputationsverluste zur Folge.

Unter Corporate Governance ist im engeren Sinne eine „verantwortungsvolle Unternehmensführung und Kontrolle“ zu verstehen (vgl. Hoffmann Consult o. J, S. 3). Eine detailliertere Definition von Corporate Governance ist hierbei nicht so leicht vorzunehmen, wie es auf den ersten Blick scheint. Unterschiedliche nationale und internationale Rechtsquellen bilden die Grundlage der Corporate Governance, wobei jedoch eine stark abweichende Verwendung der dazugehörigen Begriffe zu verzeichnen ist. Nach einer deutlich weiter gefassten Definition ist Corporate Governance die „verantwortliche und auf nachhaltige Wertschöpfung gerichtete Leitung und Kontrolle von Unternehmen und Konzernen, die sowohl nach dem jeweiligen Gesetz geltende Funktionszuweisungen und Pflichten einbezieht als auch zusätzliche Grundsätze, deren freiwillige Beachtung zunehmend als ein wichtiger Bestandteil wertorientierter Unternehmensführung verstanden wird“ (Meister 2007, S. 8). Meister bezieht sich dabei auf die ursprüngliche britische Definition von Corporate Governance aus dem Cadbury Report des Jahres 1992. In dieser Definition sind weitere Kernelemente des Corporate Governance enthalten, wie zum Beispiel das Einhalten von geltenden Rechtsgrundlagen, aber auch das freiwillige Einrichten von Systemen und Denkansätzen, um Corporate Governance als tatsächlichen Mehrwert im Unternehmen zu verankern. Gerade dieser zweite Punkt findet sich immer mehr in aktuellen Diskussionen wieder, da Unternehmen unabhängig von gesetzlichen Vorgaben und anwendbaren Richtlinien bestrebt sind, eine Corporate Governance-Kultur zu etablieren. Durch das Thema Corporate Governance ergeben sich zudem Anforderungen an die Unternehmensfunktionen und auch an entsprechende Interessengruppen, den Stakeholdern. Neben den Eigentümern und Vorständen haben auch andere Institutionen und Gruppen Einfluss auf Entscheidungsprozesse und das Tagesgeschäft (vgl. Hofmann Consult o. J, S. 4). Ein Unternehmen wird dabei von vielen Stakeholdern direkt oder indirekt beeinflusst. Die eigentliche Notwendigkeit von Corporate Governance resultiert in erster Linie aus der Trennung von Eigentum und Kontrolle, der sogenannten Principal-Agent Theory (vgl. Meister 2007, S. 6). Die Principal-Agent Theory steht dabei im Kontrast zum Shareholder-Value Ansatz, welcher den Anteilseigner beziehungsweise den Aktionär in

den Mittelpunkt aller unternehmerischen Entscheidungen rückt. Anders als im Shareholder-Value Ansatz besagt die Theorie, dass in Unternehmen heute größtenteils eine Delegation von Verantwortung an Dritte vorzufinden ist. Dabei bezeichnet „Principal“ einen Auftraggeber und „Agent“ einen Beauftragten. Das Problem bei einer solchen Delegation liegt in der Informationsasymmetrie bzw. der nicht vollständig übereinstimmenden Interessenslage zwischen Prinzipal und Agent. Corporate Governance kann hierbei als Instrument zur Beseitigung von Problemen zwischen Prinzipal und Agent angesehen werden (vgl. Meister 2007, S. 7). Corporate Governance versucht darüber hinaus, Verhaltensregeln zu definieren und Stakeholdern die Möglichkeit zu opportunistischem, also für das Unternehmen nachteiligem Handeln zu nehmen (vgl. Rohlfs 2019, S. 34).

12.1.2 Compliance

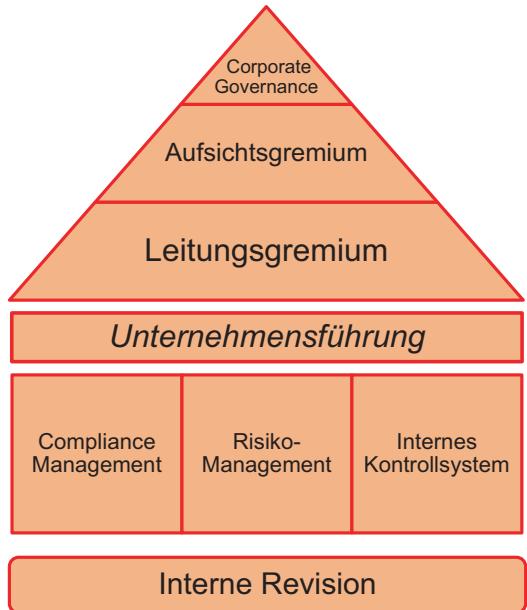
Compliance beinhaltet eine Konkretisierung des oben beschriebenen Corporate Governance-Ansatzes. Es handelt sich dabei um die Einhaltung von gesetzlichen Vorgaben sowie unternehmensinternen und -spezifischen Richtlinien. Compliance ist damit ein Soll-Zustand, der Gesetzes-, Regel- und Vertragskonformität anstrebt (vgl. Gruber et al. 2014, S. 103). Compliance-Risiken bewegen sich damit auf einem abstrakteren Niveau als die operativen Risiken eines Unternehmens. Dies liegt auch daran, dass sich die Rechtsfolgen für die handelnden Personen nicht immer von selbst erschließen. So wurde Compliance lange als eine Aufgabe betrachtet, die primär von Juristen, das heißt von der Rechtsabteilung des Unternehmens, zu lösen sei (vgl. Kark 2013, S VII). Die damit einhergehenden Risiken betreffen jedoch ein breit gefächertes Spektrum und sind daher nicht nur als „juristische Aufgabe“ zu betrachten.

Compliance ist als Unterrubrik des Corporate Governance zu verstehen. In Abb. 12.1 ist ein beispielhaftes Modell eines der führenden Wirtschaftsprüfungs- und Beratungsunternehmen in Deutschland dargestellt. Im Modell „House of Governance“ wird deutlich, dass die wesentlichen Elemente des Corporate Governance das Risikomanagement im klassischen Sinne, das interne Kontrollsyste (IKS) und auch das hier beschriebene Compliance Management sind. Compliance ist eine eigenständige Komponente der Unternehmensführung, die in der weiteren Ausarbeitung betrachtet werden soll.

12.1.3 Compliance im betrieblichen Risikomanagement

Die Compliance-Funktion spielt überwiegend im Prozessschritt der Risikokontrolle eines Unternehmens eine zentrale Rolle. Die Risikokontrolle befasst sich dabei mit der „laufenden Überprüfung der Wirksamkeit und Effizienz des Risikomanagements“ (Rohlfs 2019, S. 302). Bei der Risikokontrolle wird grundsätzlich zwischen prozessintegrierten und prozessunabhängigen Überwachungs- bzw. Kontrollmaßnahmen unterschieden. Da sich Compliance nicht dezidiert an einzelne Prozesse knüpfen lässt, ist es im Teilsegment der

Abb. 12.1 House of Governance. (Quelle: eigene Darstellung)



prozessunabhängigen Kontrolle angesiedelt. Während der Aspekt Controlling im Zusammenhang mit prozessbegleitender und weisungsgebundener Kontrolle verwendet wird, ist im Bereich der prozessunabhängigen Überwachung der Begriff des internen Kontrollsyste ms von größter Bedeutung (vgl. Gruber et al. 2014, S. 103). Dabei ist Compliance als ein integraler Bestandteil des internen Kontrollsyste ms zu verstehen. Dies lässt sich exemplarisch an dem Modell „Three-Lines-of-Defence“ demonstrieren, welches die Grundlage für ein funktionierendes Corporate Governance System darstellt. Während die erste Verteidigungslinie sich auf das operative Tagesgeschäft fokussiert, ist Compliance Bestandteil der zweiten Verteidigungslinie und damit Teil des Linienmanagements. Es dient dazu, Kontrollen auszubauen und die handelnden Personen aus der ersten Verteidigungslinie zu überwachen sowie zu überprüfen, ob die operative Geschäftsebene die Anforderungen an gesetzeskonformes Verhalten erfüllt. Die interne Revision als dritte Verteidigungslinie stellt hingegen eine übergeordnete, unabhängige Kontrollinstanz dar, die auf die ersten beiden Verteidigungslinien Bezug nimmt. Hier wird deutlich, dass Compliance als Teil der zweiten Verteidigungslinie Bestandteil des internen Kontrollsyste ms ist. Das Modell der „Three-Lines-of-Defence“ ist exemplarisch in Abb. 12.2 dargestellt.

Um Compliance-Risiken jedoch tatsächlich kategorisieren zu können, werden sie typischerweise (wie andere Risiken im Unternehmen) in der Risikolandkarte des Unternehmens (Risikomatrix bzw. Risk Map) dargestellt.

Neben der Risikokontrolle findet Compliance Management somit auch im Bereich der Risikobewertung des Risikomanagementprozesses statt. Hierbei sind die entscheidenden Parameter zur Quantifizierung des Risikos die Eintrittswahrscheinlichkeit und das Schadensausmaß. Abb. 12.3 zeigt beispielhaft eine solche Risk Map. Der Mehrwert der Darstellung in einer Risikomatrix liegt vor allem darin, dass Compliance Risiken durch

Abb. 12.2 Three Lines of Defense. (Quelle: eigene Darstellung)

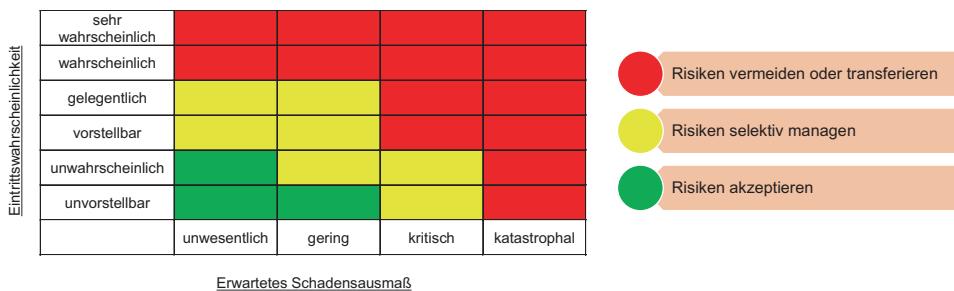
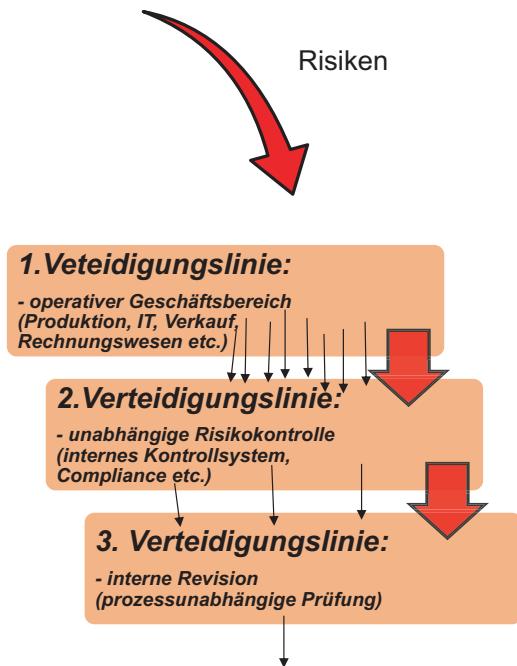


Abb. 12.3 Risikomatrix. (Quelle: eigene Darstellung)

die Darstellung des Schadensausmaßes auf der Abszisse eine quantitative Komponente erhalten. Dies spielt dann eine große Rolle, wenn es darum geht, welche finanziellen Auswirkungen ein Unternehmen bei Compliance-Verstößen zu befürchten hat. Die Themen Non-Compliance und Haftungsfragen werden später detaillierter betrachtet.

12.2 Rechtliche Grundlagen und wesentliche Rechtsquellen im Compliance-Bereich

Die Themen Corporate Governance und Compliance sind in zahlreichen internationalen und nationalen Rechtsquellen geregelt. Seit Anfang der Neunzigerjahre wurden etliche Bestimmungen erlassen, die den Zweck hatten, für Unternehmen einen Compliance-

Rahmen zu schaffen. Im Folgenden werden die wesentlichen Rechtsquellen und ihre Funktion für die Unternehmensführung erläutert.

12.2.1 Sarbanes-Oxley Act (SOX)

Anders als in Deutschland ist Corporate Governance in den USA seit jeher ein Bestandteil einschlägiger Lehrbücher zum Thema Unternehmensstrategie (vgl. Hoffmann Consult o. J, S. 5). Als Folge verschiedener Korruptionsfälle und daraus resultierender Bußgelder um die Jahrtausendwende wurde im Jahr 2002 der Sarbanes-Oxley Act erlassen. Dieses Gesetz steht vor allem für eine bessere Kontrolle im Unternehmen hinsichtlich der handelnden Personen und der unternehmensspezifischen Prozesse. Es wurde erlassen, um den Anlegerschutz zu verbessern und Unternehmensinformationen genauer und verlässlicher darzustellen. Die Implementierung der Vorgaben des Sarbanes-Oxley Acts bedeutete für Unternehmen in den USA zwar erheblichen Aufwand, brachte jedoch erhebliche Vorteile für die Compliance-Risikosituation und erleichterte die Identifizierung von Compliance-Risiken (vgl. Kark 2013, S. 115). Unmittelbare Relevanz hatte das Gesetz jedoch nur für deutsche Tochterunternehmen amerikanischer Konzerne, die an der amerikanischen Wertpapierbörsen gehandelt wurden. Allerdings gingen die Anforderungen an interne Kontrollsysteme und Risikomodelle in den USA so weit über die Standards in Deutschland hinaus, dass die Gesetzgebung des Sarbanes-Oxley Acts starke Auswirkungen auf die Entwicklung der Themen Corporate Governance und Compliance in Deutschland hatte. Vor allem der Begriff Compliance wurde aus dem amerikanischen Kontext übernommen (vgl. Gruber et al. 2014, S. 32). Noch heute wird der Sarbanes-Oxley Act als internationaler Vergleichsmaßstab herangezogen, auch wenn er außerhalb der USA keine unmittelbare Rechtswirkung hat.

12.2.2 Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)

Das KonTraG ist einer der ersten Entwicklungsschritte einer modernen Corporate Governance und damit auch seiner konkreten Ausgestaltung für Compliance im Unternehmen (vgl. Rohlfs 2019, S. 34). Es trat zum 01.05.1998 in Kraft und beinhaltet im Wesentlichen eine Änderung des Aktiengesetzes. Im allgemeinen Gesetzesentwurf hieß es, dass durch das KonTraG Schwächen und Verhaltensfehlsteuerungen korrigiert werden sollten, um mehr Transparenz und Publizität in allen Bereichen zu schaffen (vgl. Kark 2013, S. 6). Durch das KonTraG wurde eine rechtliche Dimension für das Thema Risikofrüherkennung geschaffen. Gemäß § 91 Abs. 2 AktG hat der Vorstand die Verpflichtung, geeignete Maßnahmen zu treffen, um die Überwachung im Unternehmen zu gewährleisten. Insbe-

sondere wird hierbei auf das Thema Organisation eingegangen. Ob der Vorstand seinen Aufgaben im Rahmen des § 91 Abs. 2 AktG. nachgekommen ist, hat der Wirtschaftsprüfer im Rahmen seiner alljährlichen Abschlussprüfung zu beurteilen. Es ist unschwer zu erkennen, dass die Verpflichtung nach § 91 Abs. 2 AktG wenig konkret gefasst ist. Nicht einmal der Begriff „Risiko“ wurde verwendet. Auch die Art und Weise, wie der Vorstand mit bestandsgefährdenden Entwicklungen umzugehen hat, bleibt ungeregelt (vgl. Romeike 2008, S. 6). Darüber hinaus ergibt sich nach § 76 Abs. 1 AktG die Leitungspflicht des Vorstands. Diese besagt, dass der Vorstand verantwortlich für die betrieblichen Geschäfte ist. Hierzu gehört die Pflicht, Schäden für die Gesellschaft zu verhindern (vgl. Romeike 2008, S. 11). Die Haftungsperspektive des Vorstands wird dabei später genauer beurteilt. Die Frage nach einer möglichen Pflichtverletzung ist allerdings sehr genau zu betrachten, da neben dem Gesetz auch die üblichen Verkehrskreise des Vorstands und damit das individuell von ihm betriebene Geschäft beachtet werden muss. Es ist nichtsdestotrotz unerlässlich, von einem verantwortungsbewussten Vorstand zu verlangen, ein System zur Risikofrüherkennung zu implementieren.

12.2.3 Deutscher Corporate Governance Kodex (DCGK)

Der DCGK wurde im Jahr 2002 ins Leben gerufen und soll das Thema Corporate Governance in Deutschland transparenter und verbindlicher machen. Vor allem soll der Kodex die im Jahr 1998 ins Leben gerufenen Handlungsanweisungen des KonTraG konkretisieren. Er ist jedoch eher als eine Art Leitfaden zu verstehen, da er Handlungsempfehlungen an die verantwortlichen Personen (überwiegend der Vorstand und der Aufsichtsrat) gibt. Auch wenn der DCGK vordergründig nur für börsennotierte Unternehmen gilt, haben seine Regelungen im allgemeinen Verständnis von Corporate Governance allgemeingültigen Charakter (vgl. Rohlfs 2019, S. 34). Der einzige tatsächlich verpflichtende Teil des DCGK ist die gemäß § 161 AktG zu verfassende Entsprechungserklärung, wobei Vorstand und Aufsichtsrat verpflichtend darlegen müssen, ob sie den Empfehlungen der Regierungskommission des DCGK entsprochen haben oder in welchem Umfang dies unterblieben ist. Konkrete Begründungen müssen allerdings nicht erbracht werden. Diese Erklärung ist zudem den Aktionären dauerhaft zugänglich zu machen (vgl. Hofmann Consult o. J, S. 6). Durch diese quasi-normative Ebene enthält der Kodex einen teilweise verbindlichen Charakter. Der Kodex wird jährlich durch die Regierungskommission überprüft und angepasst. Ziel des DCGK ist es, den deutschen Unternehmen Regeln an die Hand zu geben, um eine gute und verantwortungsvolle Unternehmensführung zu implementieren. Auch wenn es sich beim Deutschen Corporate Governance Kodex nicht um bindendes Recht handelt, so muss sich jedes Vorstandsmitglied mit den Inhalten auseinandersetzen. Von Wirtschaftsprüfern wird der DCGK indes als eine Art best-practice verstanden und dort als Vergleichsmaßstab herangezogen, wo das Gesetz nicht hinlänglich kodifiziert ist bzw. dort, wo ein Ermessensspielraum besteht.

12.2.4 Weitere Rechtsquellen

Das Thema Compliance ist in vielen weiteren Rechtsquellen von zentraler Bedeutung. Das Bilanzrechtsmodernisierungsgesetz (BilMoG), das Kapitalanlagegesetzbuch (KAGB) und das Wertpapierhandelsgesetz (WpHG) sind nur einige dieser rechtlichen Eckpfeiler. Speziell für den Versicherungsbereich ist das Versicherungsaufsichtsgesetz (VAG) zu nennen, das seit 2016 die Compliance-Funktion im Rahmen des internen Kontrollsystems regelt (§ 29 VAG). Danach müssen Versicherungsunternehmen im Rahmen des internen Kontrollsystems über eine Funktion zur Überwachung der Einhaltung der Anforderungen verfügen. Zu den Aufgaben der Compliance-Funktion gehört die Beratung des Vorstands in Bezug auf die Einhaltung der Gesetze und Verwaltungsvorschriften, die für den Betrieb des Versicherungsgeschäfts gelten. Außerdem hat die Compliance-Funktion die möglichen Auswirkungen von Änderungen des Rechtsumfeldes für das Unternehmen zu beurteilen und das mit der Verletzung der rechtlichen Vorgaben verbundene Risiko (Compliance-Risiko) zu identifizieren und zu beurteilen.

Im Grundsatz knüpfen die hier exemplarisch genannten weiteren Rechtsquellen bis heute an den Rechtsgedanken der vorher genannten Vorschriften an.

12.3 Compliance Management System (CMS)

Unter einem Compliance Management System (CMS) sind die auf der Grundlage der vom Vorstand festgelegten Ziele und eingeführten Grundsätze sowie Maßnahmen eines Unternehmens zu verstehen, die auf die Sicherstellung eines regelkonformen Verhaltens der gesetzlichen Vertreter und der Mitarbeiter des Unternehmens ggf. von Dritten abzielen. Das Einhalten bestimmter Regeln und die Verhinderung wesentlicher Regelverstöße spielen dabei eine zentrale Rolle (vgl. Rohlfs 2019, S. 45). Im deutschen Recht gibt es keine konkrete Vorgabe und auch keine Rechtspflicht, ein CMS einzurichten. Allerdings weisen das BilMoG und der DCGK explizit auf die Plichten der leitenden Personen (Vorstand und Aufsichtsrat) und die Einhaltung gesetzlicher Bestimmungen hin. Im Jahre 2011 wurde zudem der „Standard zur Prüfung von Compliance Management Systemen“ des Instituts für Wirtschaftsprüfer (IDW) veröffentlicht. Dieser Standard richtet sich an Wirtschaftsprüfer und bildet den Maßstab dafür, unternehmensinterne Compliance Systeme zu bewerten. Aber auch für Unternehmen ist der Standard von großer Bedeutung, da er in der allgemeinen Praxis als Vergleichsmaßstab herangezogen wird, ob und in welchem Umfang das Unternehmen seinen Sorgfalts- und Organisationspflichten nachgekommen ist (vgl. Kunz 2011). In den letzten Jahren hat sich ein einheitliches System etabliert, welches von einer Haftung des Unternehmens absieht, sofern ein CMS nach dem IDW Standard (IDW PS 980) eingerichtet wurde. Bei der Implementierung eines solchen CMS ist auf die bestehende Unternehmensorganisation und auf individuelle Gegebenheiten im Unternehmen Rücksicht zu nehmen. Ein aufwendiges Compliance-System löst für das jeweilige Unternehmen zwar Kosten aus, bietet allerdings auch den Mehrwert, das Risiko von

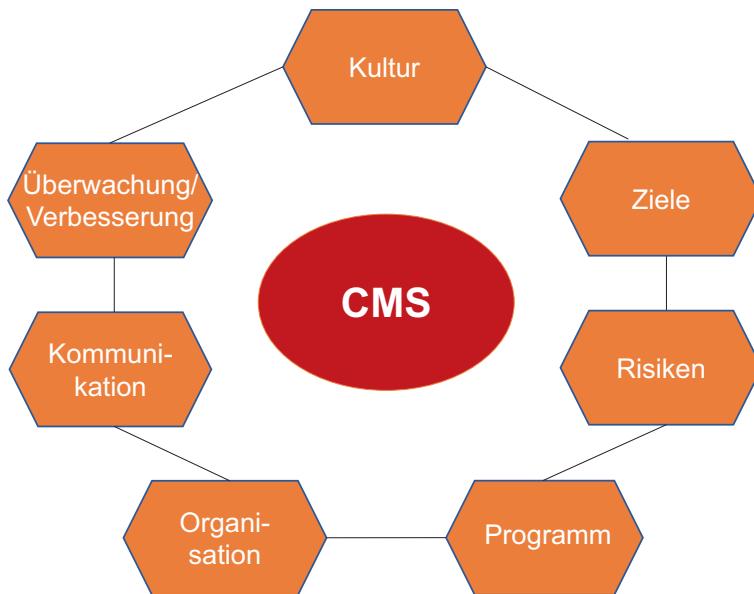


Abb. 12.4 Compliance Management System. (Quelle: eigene Darstellung)

Compliance-Verstößen zu minimieren. So bietet das CMS Vorteile, die sogar dazu beitragen können, den Unternehmenswert zu steigern. Ziel des CMS ist es, systematische Voraussetzungen zu schaffen, sodass Verstöße gegen Compliance-Anforderungen vermieden bzw. deutlich erschwert werden (vgl. TÜV Rheinland 2011, S. 6). Ein angemessenes CMS nach dem aktuellen Prüfungsstandard des IDW (IDW PS 980) weist insgesamt sieben miteinander in Wechselwirkung tretende Grundelemente auf. Abb. 12.4 stellt eine beispielhafte Veranschaulichung eines CMS dar. Im Folgenden findet eine kurze Umschreibung all dieser sieben Elemente statt.

12.3.1 Kultur

Ausgangspunkt jedes CMS ist die Compliance-Kultur im Unternehmen. Diese bildet die Grundlage für die Angemessenheit und Wirksamkeit eines CMS (vgl. IDW PS 980, Tz. 23). Sie ist ein geeigneter Gradmesser, um festzustellen, wieviel Bedeutung das Unternehmen der Regeltreue und Gesetzeskonformität beimisst. Hat ein Unternehmen eine gute Compliance-Kultur, fällt es den Mitarbeitern leichter, aus Compliance-Sicht relevante Regeln zu akzeptieren und zu befolgen. Eine gute Compliance-Kultur zeichnet sich durch eine ausgeprägte Vorbildfunktion des Managements und der Aufsichtsorgane aus. In diesem Sachzusammenhang fällt oft der Begriff des „tone at the top“. Diese Bezeichnung ist auf eine Unternehmensphilosophie zurückzuführen, die sowohl von verbalen als auch von vorgelebten Bekenntnissen des Vorstands und der leitenden Organe ausgeht. Diese Vor-

bildfunktion soll einen direkten Einfluss auf die Mitarbeiter haben. Das „Commitment“ der Leitungsorgane ist dabei unentbehrlich. Zusätzlich dazu bietet sich eine verbindliche Formulierung von Ethik-Richtlinien als Code of Conduct an (vgl. Schulz 2014). Damit werden Wertvorstellungen und Regeln schriftlich festgehalten und es wird Klarheit für alle Beteiligten geschaffen. Allerdings müssen die schriftlich festgehaltenen Werte und Vorstellungen im Unternehmen tatsächlich gelebt werden, damit von einer guten Compliance-Kultur gesprochen werden kann.

12.3.2 Ziele

Die Compliance-Ziele eines Unternehmens sollten immer Bezug auf die Unternehmensziele nehmen, damit eine Zielerreichung an die Strategie des Unternehmens geknüpft ist. Die betriebswirtschaftlichen Ziele werden dabei um die Compliance-Ziele ergänzt und somit erweitert (vgl. Kark 2013, S. 153). Da die betriebswirtschaftlichen Ziele vom Vorstand (ggf. unter Beteiligung des Aufsichtsrats) an jede einzelne Unternehmenseinheit weitergegeben werden, sollte mit den Compliance-Zielen ähnlich verfahren werden. Durch die Integration in eine Zielvereinbarung zusammen mit den genannten betriebswirtschaftlichen Zielen tragen die Führungskräfte selbst und nicht eine zentrale Compliance-Stelle im Unternehmen für die Rechtmäßigkeit der operativen Prozesse die Verantwortung (vgl. Kark 2013, S. 151). Der IDW Standard PS 980 stellt hierbei Anforderungen an die Compliance-Ziele eines Unternehmens. Konsistenz, Verständlichkeit, Messbarkeit und eine ausreichende Abstimmung der Ziele mit den verfügbaren Ressourcen werden hierbei explizit hervorgehoben (vgl. IDW PS 980, Tz. 23, A14).

Compliance hat mehrere Funktionen im Unternehmen. In erster Linie soll Compliance die Aufgabe erfüllen, Haftungsansprüche vom Unternehmen fernzuhalten (Haftungsbegrenzungsfunktion). Dazu können ebenso Bereiche wie das Kartellrecht und die Korruptionsbekämpfung, aber auch die sogenannte Tax-Compliance gehören. Im Rahmen der Tax-Compliance ist es wichtig für das Unternehmen, steuerliche Verpflichtungen vollständig und zeitgerecht zu erfüllen, da sonst finanzielle, strafrechtliche oder reputative Konsequenzen drohen können. Auch aus dem Kartellrecht folgen Compliance-Ziele. Hier sind vor allem das Gebot eigenständigen Marktverhaltens und das Abstimmungsverbot zu nennen, da die rechtlichen Konsequenzen von Verstößen sehr weitreichend sein können. Für die meisten Unternehmen ist das Kartellrecht daher auch der wichtigste Baustein im Compliance-Management. Die verschärzte Bußgeldpraxis in der jüngsten Vergangenheit unterstreicht diese Notwendigkeit. Neben der Haftungsbegrenzungsfunktion hat Compliance weitere Ziele. So setzt sich ein CMS darüber hinaus auch das Ziel, ein Unternehmensimage aufzubauen, welches vertrauensvoll und regelkonform wirkt (Imagefunktion). In Ergänzung dazu kommt die Kontrollfunktion von Compliance zum Tragen, da das Unternehmen stets bemüht sein sollte, die Compliance auch der Entscheidungsträger zu monitoren, um keine Nachteile durch Non-Compliance zu „starker“ Einzelpersonen im Unternehmen zu erleiden. Die hier beschriebenen Compliance-Ziele bilden dabei gleichzeitig die Basis für das nächste Grundelement eines CMS, die Compliance-Risiken.

12.3.3 Risiken

Im Zusammenhang mit Compliance-Fragen ist besonders die Risikoidentifikation bedeutsam. Ganz generell lassen sich Risiken im Bereich Compliance in verschiedene Untergruppen einteilen, beispielsweise Produktrisiken, Kundenrisiken, Mitarbeiterrisiken, aber auch Transaktions- und die genannten Rechtsrisiken. Korruptions-, Kartell- und Vermögensrisiken gelten als die klassischen Compliance-Risiken. Zur Identifikation werden Verfahren zur systematischen Risikoerkennung benötigt, um ein Risiko hinsichtlich der Höhe und des Ausmaßes zu beurteilen (vgl. IDW PS 980, Tz. 23). Ein probates Mittel ist dabei die in der vorherigen Abbildung dargestellte Risikomatrix. In diesem Zusammenhang stellt sich die Frage, wie der rechtliche Rahmen, die unternehmensindividuelle Risikolage und das nähere Umfeld aussehen. Eine wichtige Kennziffer im Bereich der Compliance-Risiken ist ferner das Rating. Auch dieses kann darüber Aufschluss geben, wie ein Unternehmen das Thema Compliance bewertet. So führen nicht selten grobe Compliance-Verstöße zu einer Ratingabstufung oder zumindest zu einer kritischen Anmerkung seitens der Ratingagenturen. Klassische Unternehmensrisiken kann die Ratingagentur aus der Gewinn- und Verlustrechnung, Kontobewegungen, internen Kennzahlen oder anhand vorhandener Branchenkenntnisse zumindest abschätzen. Beim Compliance-Risiko ist dies deutlich schwieriger (vgl. Kark 2013, S. 43). Allein das Vorhandensein eines ausgereiften Compliance-Management-Systems zeigt jedoch, dass sich das Unternehmen intensiv mit seinen Compliance-Risiken befasst hat. Ohne die Implementierung eines solchen Systems könnte sich eine Ratingagentur nur am Branchenstandard orientieren und eine Pauschalbewertung abgeben. Die transparente Darstellung der Compliance-Risiken könnte zu einem besseren Rating führen, da gezeigt werde, dass Risikofrüherkennung, Risikoidentifikation und auch der Umgang mit Compliance-Risiken für das Unternehmen wichtig sind (vgl. Kark 2013, S. 43).

Neben der Identifikation der Risiken ist die Risikoanalyse von großer Bedeutung. Bereits erkannte Risiken müssen kategorisiert und gemäß der bekannten Risikosteuerungsmaßnahmen des klassischen Risikomanagementprozesses behandelt werden. Dies sind neben der Risikoverminderung, der Risikovermeidung und dem Risikotransfer auch das bewusste Selbsttragen eines Risikos (vgl. Rohlfs 2019, S. 256). Ein häufiges Problem bei der Bewertung von Compliance-Risiken liegt bei bereits erfolgter Risikoidentifikation darin, dass ein quantitatives Ausmaß oftmals nur schwer abschätzbar ist. Gerade bei Korruptionsfällen und den damit verbundenen Reputationsrisiken sind finanzielle Folgen oft nur indirekt antizipierbar. Verstöße resultieren dabei aus individuellem oder kollektivem Fehlverhalten, teilweise sogar durch Beteiligung von externen Dritten. Zudem ist es wichtig, alle Compliance-Risiken zu dokumentieren. Dies dient dazu, eine Anpassung des CMS an sich ständig wandelnde Anforderungen zu ermöglichen. Dies gewinnt vor allem dann Bedeutung, wenn der Prozess der Compliance-Risiko-Steuerung bewertet und kritisch hinterfragt werden soll.

12.3.4 Programm

Das Compliance-Programm wird auf der Grundlage der zuvor erfolgten Beurteilung von Compliance-Risiken erstellt (vgl. IDW PS 980, Tz. 23). An dieser Stelle werden bereits Grundsätze und Maßnahmen konkret formuliert, damit es möglichst nicht zu einem Compliance-Verstoß im Unternehmen und den daraus resultierenden Folgen kommt. Dabei sollen jegliche Maßnahmen stets einen präventiven Charakter haben (vgl. Romeike 2008, S. 19). Das übergeordnete Ziel eines Compliance-Programms ist das rechtzeitige Erkennen von Verstößen und darüber hinaus eine antizipative Komponente für mögliche künftige Regelverstöße. Eine spürbare Präventionswirkung kann vor allem auch durch den Einsatz eines Compliance-Managers erzielt werden. Dies liegt daran, dass allein schon durch die bloße Existenz einer solchen Funktion bzw. Person das Bewusstsein für bestehende Haftungsrisiken deutlich gesteigert wird (vgl. Romeike 2008, S. 111). Ein Compliance-Programm ist zu dokumentieren, um eine jederzeitige Überprüfbarkeit zu gewährleisten. Mögliche Maßnahmen eines solchen Compliance-Programms sind beispielsweise Job-Rotationen, Funktionstrennungen, Sicherheitskontrollen aber auch ganz spezifische Handlungsanweisungen für einzelne Personen oder Personengruppen. Die Ziele eines ausgereiften Compliance-Programms lassen sich in diesen drei Punkten zusammenfassen (vgl. Hans Böckler Stiftung 2011, S. 21):

1. Compliance-Verstöße zu verhindern (Prevention);
2. Regelverstöße schnellstmöglich zu erkennen (Detection);
3. auf Verfehlungen so schnell wie möglich eine Reaktion zu zeigen (Response).

Wichtig ist, dass Compliance-Programme sich nicht auf theoretische Ausführungen beschränken, sondern auch Hinweise zur operativen Umsetzung geben. Gute Compliance-Programme zeichnen sich dadurch aus, dass sie passgenau für das jeweilige Unternehmen sind und von der Unternehmensspitze aus bis in die kleinste Unternehmenseinheit transportiert werden. Wichtig ist ferner, dass ein Compliance-Programm neben den rechtlichen auch die wirtschaftlichen Komponenten berücksichtigt.

12.3.5 Organisation

Ein weiterer integraler Bestandteil eines CMS ist eine wirksame Aufbau- und Ablauforganisation. Hierbei sind verschiedene Ausgestaltungsformen denkbar. Entweder richtet ein Unternehmen eine eigene Stabstelle als Compliance-Abteilung ein oder es überträgt das Thema Compliance an die Rechtsabteilung (vgl. Hans Böckler Stiftung 2011, S. 23). In jedem Fall bedarf es genauer Absprachen und klarer Zuständigkeiten zwischen den jeweiligen Abteilungen. In größeren Unternehmen werden Leitungsaufgaben meist bis in die

zweite oder dritte Managementlinie verlagert. Gerade hier spielt die Organisationspflicht eine große Rolle, da keinem Vorstand zugemutet werden kann, jeden einzelnen Mitarbeiter bis ins letzte Detail zu kontrollieren. Dies ist auch der Grund dafür, warum Vorstandsmitglieder tendenziell nicht für das Verschulden der Mitarbeiter, allerdings für das fehlende bzw. fehlerhafte Einrichten einer Compliance-Organisation, haften (vgl. Romeike 2008, S. 22). Gemäß des IDW Standards zeichnet sich eine gute Compliance-Organisation in erster Linie durch klare Guidelines hinsichtlich der Festlegung von Verantwortlichkeiten und Rollen im Unternehmen aus. Sofern Pflichten auf mehrere Organisationseinheiten oder Personen verteilt werden, besteht immer auch das Risiko einer Kompetenzüberschneidung bzw. unklarer Kompetenzen. Verlässt sich hier eine Person auf die andere, können dadurch folgenschwere Umsetzungs- bzw. Überwachungslücken entstehen (vgl. Gruber et al. 2014, S. 39). Darüber hinaus müssen ausreichend Ressourcen zur Verfügung gestellt werden und das CMS sollte in andere bestehende Unternehmenssysteme, etwa in eine bereits bestehende Ablauforganisation oder den bereits existierenden Risikomanagementprozess, integriert werden (vgl. IDW PS 980, Tz. 23, A18). Auch das Einrichten einer separaten „Whistleblower-Hotline“ wird von vielen Standards empfohlen, um eine zusätzliche Anlaufstelle für eine nachhaltige Korruptionsbekämpfung zu bieten. Am geeigneten scheinen dabei Systeme, bei welchem ein anonymes Hinweisgebersystem angewandt wird. Gerade auch vor dem Hintergrund, Hinweisgeber vor innerbetrieblichen Konsequenzen zu bewahren.

12.3.6 Kommunikation

Das Grundelement einer ausreichenden Compliance-Kommunikation ist die Informationsweitergabe der bereits beschriebenen Erfassung der Compliance-Risiken und damit auch der Inhalte des Compliance-Programms an die Mitarbeiter. Klare Zuweisungen der Kompetenzen und Verantwortlichkeiten durch eine transparente und unmissverständliche Kommunikation sind dabei von entscheidender Bedeutung. Gemäß des IDW Prüfungsstandards sind besonders die anlassabhängigen und -unabhängigen Berichtspflichten des Unternehmens, die Berichtswege bei vermuteten Compliance-Verstößen und die Kommunikation an die zuständigen Stellen im Unternehmen, aber ggf. auch an Behörden, wichtig (vgl. IDW PS 980, Tz. 23, A19). Auch Compliance-Schulungen und Kommunikationskampagnen können für das individuelle Unternehmen sinnvoll sein. Diese müssen dann aber auch auf bestimmte Zielgruppen im Unternehmen zugeschnitten sein (vgl. KPMG (o. J.), S. 5). Ziel des gesamten Prozesses ist es, unternehmensintern ein Risikobewusstsein für Compliance-Verstöße zu etablieren. Außerdem spielt eine gute Compliance-Kommunikation im Zusammenhang mit dem Datenschutz und der IT-Compliance eine übergeordnete Rolle.

12.3.7 Überwachung und Verbesserung

Im Zuge der Überwachung und Verbesserung eines CMS wird vom Monitoring-Instrument gesprochen. Hierzu zählen das Einrichten eines Hinweisgebersystems, Compliance-Audits und regelmäßige Berichterstattungen an den Aufsichtsrat und den Vorstand (vgl. KPMG (o. J.), S. 5). Beim Thema Überwachung sollte darüber hinaus der Fokus auf eine prozessunabhängige Kontrolle gelegt werden, damit das Monitoring unverfälscht und unvoreingenommen ablaufen kann. Eine Alternative dazu ist eine externe Überwachung durch einen externen Dienstleister. Diese Option muss jedoch immer auch eine Kostenabwägung beinhalten. Die Ergebnisse dieser Überwachungsmaßnahmen werden darauf verwendet, Schwachstellen im Unternehmen aufzudecken und auch gleichzeitig gegensteuernde Prozesse einzuleiten (vgl. IDW PS 980, Tz. 23, A20). Die wohl bedeutsamste Maßnahme ist das Erstellen von internen Richtlinien und allgemeinen Verhaltensaufforderungen an die Mitarbeiter. An dieser Stelle kommen aber auch andere Maßnahmen in Betracht, wie etwa die qualifizierte Mitarbeiterschulung. Hierzu gehören auch Konsequenzen für nicht compliant handelnde Mitarbeiter. Die Organisation muss über Abläufe verfügen, die den Compliance-Anforderungen Rechnung tragen kann. Angemessene Maßnahmen müssen daher immer die interne Organisation und somit auch die Strukturen des Unternehmens berücksichtigen (vgl. TÜV Rheinland 2011, S. 16). Dabei ist die Unternehmensleitung für die Errichtung und Aufrechterhaltung sowie die ständige Prozessverbesserung des Compliance Management Systems verantwortlich (vgl. TÜV Rheinland 2011, S. 3).

12.4 Non-Compliance und Haftungsfragen

Jeder Regelverstoß kann zu einer Haftung führen. Die Befassung mit der Haftungsfrage bei Compliance-Verstößen wirft zunächst die Frage auf, wie ein Pflichtverstoß im Bereich Compliance konkret aussieht bzw. aussehen kann. Hierzu wird zunächst der in der Literatur verwendete Begriff der „Non-Compliance“ erläutert. Anschließend wird auf die Verantwortung der handelnden Personen im Unternehmen, insbesondere die des Chief Compliance Officers (CCO) eingegangen. Sodann werden einzelne Rechtsfolgen dargestellt, die handelnde Personen bei Compliance-Verstößen treffen können.

12.4.1 Non-Compliance

Der Terminus „Non-Compliance“ beschreibt eine unzureichende Compliance-Struktur, vor allem bezogen auf die Organisation im Unternehmen. Neben dem mangelhaften organisatorischen Rahmen (Aufbau- und Ablauforganisation) ist hier auch das konkrete, nicht rechtskonforme Verhalten handelnder Personen der entscheidende Faktor. Non-Compliance

kann dabei gravierende Folgen für das Unternehmen, aber auch für das haftende Individuum haben. Wenn im weiteren Verlauf von Non-Compliance gesprochen wird, so soll hierbei lediglich das persönliche Fehlverhalten einzelner Handelnder im Unternehmen betrachtet werden.

12.4.2 Haftungssubjekte

12.4.2.1 Vorstand und Aufsichtsrat

Die Compliance-Haftung trifft wegen § 91 Abs. 2 AktG insbesondere den Vorstand. Sein unternehmerisches Ermessen wird dabei sowohl im Innen- als auch im Außenverhältnis durch die Legalitätspflicht begrenzt (vgl. Kark 2013, S. 21). Verletzt ein Vorstandsmitglied gemäß § 93 Abs. 2 AktG seine Organpflicht, so haftet er bei Vorsatz oder Fahrlässigkeit gegenüber dem Unternehmen. Neben der Kompensation des entstandenen Vermögensnachteils soll dadurch auch eine präventive Wirkung erzielt werden. Haftbar ist dabei nicht das einzelne Vorstandsmitglied, sondern der Gesamtvorstand im Wege der gesamtschuldnerischen Haftung. Demnach müssen selbst nicht-zuständige Mitglieder des Vorstands ihren Überwachungspflichten nachkommen und bei Fehlverhalten ihrer Vorstandskollegen sofort einschreiten (vgl. Romeike 2008, S. 22). Auch der Aufsichtsrat ist an diesem Prozess beteiligt. Er muss sicherstellen, dass der Vorstand seinen Berichtspflichten und Pflichten zur Errichtung eines Frühwarnsystems nachkommt. Dabei resultiert allein schon aus seiner Position als Aufsichtsrat heraus die Verpflichtung, den Vorstand zu überwachen. Er muss sich insbesondere über das Vorhandensein eines ausreichenden Systems zur Früherkennung vergewissern (vgl. Romeike 2008, S. 25). Somit ist auch der Aufsichtsrat von einer Compliance-Haftung nicht ausgenommen, soweit diesen eine schuldhafte Pflichtverletzung trifft.

12.4.2.2 Chief Compliance Officer (CCO)

Eine besondere Stellung im Bereich der Haftung nimmt der Chief Compliance Officer ein. Er ist Compliance-Verantwortlicher im Unternehmen, gilt rechtlich als Garant und bündelt die Compliance-relevanten Unternehmensbereiche in seiner Person. Er trägt ein hohes Haftungsrisiko. Im Rahmen seiner Tätigkeiten haftet er nämlich sowohl zivilrechtlich als auch strafrechtlich für sein Handeln (vgl. Compliance Academy o. J., S. 1). Ein Urteil des BGH aus dem Jahr 2009 (BGH 5 StR 394/08 – Urteil vom 17.07.2009) verankert die Garantenstellung und postuliert eine persönliche Rechtspflicht des CCO. Während der CCO persönlich strafrechtliche Konsequenzen bei einem Verstoß zu befürchten hat, kommen darüber hinaus deliktische Schadensersatzansprüche des eigenen Unternehmens in Betracht. Gerade das Risiko der Innenhaftung ist hierbei immens. Hohe Bußgelder können die Folge sein. Maßgebend dafür ist stets der Pflichten- bzw. Tätigkeitskreis, den der CCO übernimmt.

12.4.3 Rechtsfolgen

Neben allen immateriellen Konsequenzen (Reputationsverlust, Vertrauensverlust, Bruch mit ethischen Vorsätzen des Unternehmens) hat ein Compliance-Verstoß vor allem spürbare finanzielle Folgen in Form von Schadensersatzverpflichtungen und Bußgeldern. Ferner können vergaberechtliche Konsequenzen entstehen, sodass das Unternehmen behördliche Genehmigungen oder öffentliche Aufträge verliert und in Ergänzung dazu können steuerrechtliche Auswirkungen (zum Beispiel Nachzahlungen) drohen. Ein weiterer Punkt ist die mögliche Verschlechterung des Ratings oder der Kreditwürdigkeit eines Unternehmens, welches gegen Compliance-Bestimmungen verstößt. Ratingverschlechterungen oder Herabstufungen der Kreditwürdigkeit können dabei schmerzliche Auswirkungen auch auf die Liquiditätssituation und Rentabilität des Unternehmens haben (vgl. Kark 2013, S. 43).

12.5 IT-Compliance und Datenschutz

Weitere Risiken im Zusammenhang mit Corporate Governance entstehen durch die rasant voranschreitende Digitalisierung und den damit verbundenen Anforderungen an die IT-Compliance. Hinzu kommt, dass sich durch die Datenschutz-Grundverordnung, welche seit dem 25.05.2018 in Kraft ist, ein verschärftes Risikobild ergeben hat. Im Folgenden soll auf diese beiden Themen eingegangen werden.

12.5.1 IT-Compliance

IT-Compliance wird hier als separates Thema behandelt, weil es in fast allen Kernprozessen des Unternehmens einen immer größeren Stellenwert einnimmt. Nahezu alle Prozessschritte sind von einer funktionierenden IT abhängig. Die Verfügbarkeit der IT im Unternehmen bezieht sich auf Hardware und Software (vgl. Kark 2013, S. 161). IT-Compliance unterscheidet sich dabei von der Systematik und Herangehensweise kaum von der allgemeinen Compliance. Auch hier geht es um das Einhalten von gesetzlichen Vorgaben und regulatorischen Rahmenbedingungen. Allerdings liegt dabei die Anwendung bestimmter Informationstechniken im Fokus, was die Anforderungen spezifischer und auch technischer macht. Zudem werden bei der IT-Compliance relevante Schnittstellen betrachtet, wie zum Beispiel jene zu anderen Abteilungen oder zu Lieferanten (vgl. Müller und Buchsein 2016, S. 4). Sowohl in Bezug auf die Hardware als auch auf die Software ist es von großer Bedeutung, dass bei Hackerangriffen und sonstigen Ausprägungen der Cyberkriminalität durch Systeme und Analysen versucht wird, das geistige Eigentum des Unternehmens möglichst zu schützen (vgl. Kark 2013, S. 161). Die Ernennung eines Chief Information Security Officers (CISO) sollte erfolgen, um die IT-Compliance in Abstimmung

mit dem Chief Compliance Officer zu koordinieren. Im Segment der IT-Compliance sind folgende Faktoren besonders relevant:

- Lizenzmanagement
- Elektronische Archivierung
- Datensicherheit

Während durch ein umsichtiges Lizenz-Management und durch Software-Lösungen, die aktiv vor vorsätzlichen oder unabsichtlichen Datenmissbrauch schützen, ein Schutz vor finanziellen Verlusten erzielt werden kann, ist im Bereich der elektronischen Archivierung vor allem die Frage nach der Datensensibilität relevant.

12.5.2 Datenschutz

Compliance-Pflichtverstöße sind im Zusammenhang mit Datenschutz nur dann relevant, sofern es um personenbezogene Daten bzw. deren Verwendung geht (vgl. Schläger 2012, S. 1). Die zentrale Rechtsquelle in diesem Sachzusammenhang ist die EU-Datenschutzgrundverordnung (DSGVO), welche seit dem 25.05.2018 in Kraft ist. Die DSGVO will einen transparenten und bewussten Umgang mit personenbezogenen Daten regeln. Als Maßstab können hier auch die organisatorischen Verpflichtungen verwendet werden, allerdings auf einer fachlicheren und technischeren Ebene. Die Haftungsregelungen für Vorstände sind dabei ähnlich wie bei „normalen“ Compliance-Verstößen zu bewerten.

Auch in Sachen Datenschutz kann das Heranziehen eines Spezialisten haftungsmindernd wirken. So sollte ein externer Datenschutzbeauftragter ausgewählt werden, wenn Expertise oder Kapazität im eigenen Unternehmen nicht ausreichen, um die Anforderungen zu erfüllen. Der Datenschutzbeauftragte muss neben seinen juristischen Kenntnissen auch IT-bezogenes, technologisches Fachwissen aufweisen, da er an der Schnittstelle der Rechtsabteilung und der IT-Abteilung tätig ist. Wichtig ist zudem, dass sich der Vorstand auch bei Vorhandensein eines externen Datenschutzbeauftragten nicht „enthaften“ kann. Die Haftung liegt auch bei einem Verstoß gegen die DSGVO bei der Unternehmensleistung, somit beim Vorstand persönlich. Gerade im Bereich Datenschutz wollte der Gesetzgeber mit der DSGVO ein deutliches Zeichen hinsichtlich möglicher Sanktionen setzen. So soll bei Pflichtverstößen auch stets eine abschreckende Wirkung beim Unternehmen erzielt werden. Bußgelder in diesem Bereich können bis zu 20 Millionen Euro oder bis zu vier Prozent des weltweiten Jahresumsatzes des Unternehmens betragen. Die entsprechenden Regelungen finden sich in Artikel 83 DSGVO. Im Vergleich dazu waren Bußgelder im alten Bundesdatenschutzgesetz (BDSG), welches bis zur Umsetzung der DSGVO anzuwenden war, auf 50.000 Euro bzw. 300.000 Euro bei besonderen Vergehen begrenzt.

12.6 Unternehmens-Mehrwert durch Compliance

Wie bereits dargestellt wurde, ist ein ausgereiftes Compliance-System ein Mittel, um für das Unternehmen und die verantwortlichen Mitarbeiter haftungsmindernde Rahmenbedingungen zu schaffen. Des Weiteren können Bußgeldrisiken reduziert werden. Ein ausgereiftes Compliance-System im Unternehmen kann auch langfristig als Reputations- schutz angesehen werden. Durch Compliance kann ein Unternehmen dafür sorgen, das Unternehmensimage zu schützen oder sogar zu verbessern. Ein Unternehmen, welches von seinen Kunden mit guter Compliance in Verbindung gebracht wird, vermittelt das Gefühl von Verlässlichkeit und schafft Vertrauen. Auch für Lieferanten kann Compliance ein relevantes Kriterium sein, um mit einem Unternehmen in eine Geschäftsbeziehung zu treten. Somit ist Compliance auch ein Attraktivitätsfaktor (vgl. Schiffers und van der Hout 2015, S. 3). Hinzu kommt, dass durch ein ausgereiftes Compliance-System eine interne Effizienzsteigerung erzielt werden kann. Dies wird dadurch ermöglicht, dass einzelne Prozesse des Risikomanagements besser koordiniert und aufeinander abgestimmt werden können. Compliance wird somit zur Aufgabe aller Mitarbeiter, nicht nur der Organe des Unternehmens. Auch die Aufbau- und Ablauforganisation kann eine positive Veränderung dadurch erfahren, dass ein erfolgreiches CMS im Unternehmen etabliert wird. Nicht zuletzt kann durch Compliance ein ethisches Ziel verfolgt werden. Dadurch, dass Gesetzesverstöße vermieden werden, kann im Idealfall langfristig eine völlig neue Unternehmenskultur entstehen und bei allen Führungskräften und Mitarbeitern das Bewusstsein für das Thema Compliance geschaffen werden.

Literatur

- Compliance Academy GmbH. (o. J.). *Persönliche Haftung des Chief Compliance Officers (CCO) und der Compliance-Verantwortlichen*. Münster. <http://www.cco-haftung.de/>. Zugegriffen am 26.05.2019.
- Gruber, J., Günther, G., & Muschol, H. (2014). *Controlling, compliance und corporate governance*. Frankfurt a. M.: Peter Lang.
- Hans Böckler Stiftung. (2011). *Compliance – Eine Einführung in die Thematik*. https://www.boeckler.de/pdf/p_ah_ar_15.pdf. Zugegriffen am 24.05.2019.
- Hofmann Consult. (o. J.). Professionelles Know How für Unternehmensstrategien. *Corporate Governance: Welche Bedeutung hat Corporate Governance für den KMU Unternehmer*. http://www.hofmannconsult.com/Kompetenzen/Corporate_Governance.pdf. Zugegriffen am 24.05.2019.
- Kark, A. (2013). *Compliance-Risikomanagement*. München: C.H. Beck.
- KPMG. (o. J.). Compliance-Management Systeme. https://www.kpmg.de/docs/20100917_Compliance_Unternehmen.pdf. Zugegriffen am 26.05.2019.
- Kunz, J. (2011). Hilfe bei der Prüfung von Compliance-Systemen. *Stuttgarter Zeitung – Wirtschaft kompakt*, 63, 4.
- Meister, D. G. (2007). *Corporate Governance und Compliance-Management für Versicherungsunternehmen*. Saarbrücken: VDM.

- Müller , T., & Buchsein, R. (2016). IT-Compliance. *Die praktische Umsetzung von Compliance-Anforderungen.* https://www.iet-solutions.de/files/7914/6486/5958/ger_Compliance_Whitepaper_2016.pdf. Zugegriffen am 26.05.2019.
- Rohlf, T. (2019). *Risikomanagement im Versicherungsunternehmen.* Köln: VVW.
- Romeike, F. (2008). *Rechtliche Grundlagen des Risikomanagements Haftungs- und Strafvermeidung für Corporate Compliance.* Berlin: Erich Schmidt.
- Schiffers, G., & van der Hout, R. (2015). Zum Mehrwert von Compliance-Bemühungen. *Vorkehrungen lohnen sich auch für kommunale Unternehmen.* <https://publicus.boorberg.de/zum-mehrwert-von-compliance-bemuehungen/>. Zugegriffen am 26.05.2019.
- Schläger, U. (2012). *Datenschutzkonformes Compliance.* <https://www.datenschutz-notizen.de/datenutzkonformes-compliance-062822/>. Zugegriffen am 26.05.2019.
- Schulz, M. (2014). *Erfolgsfaktor Compliance-Kultur.* https://www.ggs.de/fileadmin/user_upload/Dokumente/Presse/Presseberichte/2014/ComplianceBerater-2014-4_Schulz.pdf. Zugegriffen am 24.05.2019.
- TÜV Rheinland. (2011). *Standard für Compliance Management Systeme (CMS).* <https://www.tuv.com/content-media-files/germany/bs-systems/pdfs/1214-tuv-rheinland-compliance-management-certification/tuv-rheinland-der-compliance-standard-de.pdf>. Zugegriffen am 24.05.2019.

Dr. Andreas Biegel ist Syndikusrechtsanwalt, Leiter des Geschäftsbereichs Justitiariat/Schaden und Inhaber der Compliance-Schlüsselfunktion der Delvag Versicherungs-AG in Köln. Zuvor war er Syndikus im Konzern-Justitiariat der Deutsche Lufthansa AG in Frankfurt am Main. Er ist Mitglied des Rechtsausschusses der IHK Köln und des Beirats des Deutsch-Lateinamerikanischen Studien-gangs „CALA“ der Fachhochschule Münster.

Pascal Müller studierte Versicherungswesen mit den Schwerpunkten Sachversicherung, Lebensversicherung und Personalwesen am Institut für Versicherungswesen der Technischen Hochschule Köln. Im Anschluss absolvierte er dort auch das Masterstudium Risk & Insurance. Vor dem Studium schloss er eine Ausbildung zum Kaufmann für Versicherungen und Finanzen beim Mehrfachagenten Swisslife Select ab. Als Nebentätigkeit arbeitete er während des Studiums bei einem lokalen Maklerunternehmen.



Digitalisierung & Risikomanagement

13

Markus Vorbringer und Thorben Schlätzer

Zusammenfassung

Das Risikomanagement steht wie andere Unternehmensbereiche vor einem Paradigmenwechsel. In Zeiten von Industrie 4.0, Big Data und künstlicher Intelligenz ist es schwierig zu überblicken, ob die Chancen der Digitalisierung die Herausforderungen überwiegen. Während digitale Datenströme und neue Technologien Echtzeit-Reportings und Vorhersagbarkeit potenzieller Schäden versprechen, birgt der Wechsel vom „reakтив analytischen“ hin zum „proaktiv prognostizierenden“ Risikomanagement organisatorische Herausforderungen für die Unternehmenssteuerung sowie neu zu bewertende Risiken und Kompetenzlücken, die es zu schließen gilt.

13.1 Einleitung

Der Begriff „Digitalisierung“ hat keine klare Definition, kann aber in Kurzform mit der digitalen Repräsentation analoger Informationen beschrieben werden (vgl. Luber und Litzel 2017). Die Entwicklungen aus der Digitalisierung beeinflussen nicht nur die Innovation der Weltwirtschaft durch zum Beispiel erhebliche Steigerung der Investitionen in neue Geschäftsmodelle (vgl. Ernst und Young 2019, S. 3), sondern verändern durch neue

M. Vorbringer (✉)
SAP SE, Walldorf, Deutschland
E-Mail: markus.vorbringer@sap.com

T. Schlätzer
TH Köln, Institut für Versicherungswesen, Köln, Deutschland
E-Mail: kontakt@thorbenschlaetzer.de

Technologien wie autonomes Fahren, Blockchain oder künstlicher Intelligenz die gesamte Gesellschaft.

Im Zusammenhang mit industriellem Risikomanagement ist besonders das Stichwort „Industrie 4.0“ des Öfteren zu lesen. Dessen Konzept ist vordergründig die Synchronisation digitaler Systeme mit der physischen Realität sowie die Vernetzung der Gesamtproduktion (vgl. Lasi et al. 2014, S. 261 ff.). In der Industrie entstehen vor allem durch eine immer großflächigere Vernetzung durch „Internet of Things“ (IoT), das stellvertretend für eine Infrastruktur auf Basis einer globalen Vernetzung physischer und virtueller Gegenstände steht, ganz neue Arten der Produktion (vgl. Kagermann et al. 2011, S. 2). Im Zuge dieser Entwicklungen wird daher bereits von einer vierten industriellen Revolution gesprochen, woraus der bereits genannte Begriff „Industrie 4.0“ erwächst. Diese Form der Digitalisierung soll zukünftig für Industrieunternehmen dezentrale, intelligente Systeme einsetzbar machen, die gesamte Wertschöpfungsketten selbstständig zu steuern vermögen (vgl. Ganschar et al. 2013, S. 22).

Im Zusammenhang mit steigendem Investitionsvolumen (vgl. Bitkom 2019) für diese Industrie-Revolution werden ergänzend zur gewünschten Effektivitäts- und Effizienzsteigerung der Produktion deutlich größere Datenmengen als in der Vergangenheit erhoben und verarbeitet. Diese massiven Datenmengen werden oft mit dem Begriff „Big Data“ assoziiert. Über die Daten der Produktion hinaus, versprechen sich Unternehmen Ansätze für Wettbewerbsvorteile durch datengetriebene Unterstützung strategischer Entscheidungen und ein besseres Verständnis des Marktes sowie ihrer Kunden (vgl. Dewenter und Lüth 2016, S. 649). Die Nachfrage zur Nutzung digitalisierungsbezogener Technologien führt zwangsläufig zu einer Notwendigkeit technischer Unterstützung, für die sich Unternehmen in den letzten Jahren vermehrt bei Cloud-Anbietern bedient haben, die sich den Herausforderungen technischer Weiterentwicklungen und Skalierbarkeit der immer daten hungrigeren Systeme moderner Unternehmen stellen (vgl. Gartner 2019). Anders als die Verwendung stationärer Serversysteme kann die Nutzung von Cloud-Systemen aufwändig Rechenleistungen gezielter verteilen und nach Bedarf steuern, um damit langfristige Leistungs- und Kostenvorteile auszunutzen (vgl. Avram 2014, S. 531).

Die Anknüpfungspunkte für eine veränderte Rolle des Risikomanagements ergeben sich aus den Entwicklungen der Digitalisierung und den daraus angestoßenen Innovationen, die für das Risikomanagement gleichzeitig Chancen und Herausforderungen bergen, mit denen es sich auseinanderzusetzen gilt. Wo auf der einen Seite digitalisierte Informationen den Risikomanagement-Prozess effektiver machen können, entstehen auf der anderen Seite organisatorische Veränderungen für die Unternehmen, auf die sich das entsprechende Management einstellen muss. Von Realtime-Reporting bis hin zum „Single Point of Truth“-Ansatz entstehen neue Analyse- und Steuerungsfelder für das Risikomanagement. Die Digitalisierung wird hier einen erheblichen Einfluss auf den gesamten Prozess haben. In der Folge wird analysiert, inwieweit die Digitalisierung für das Risikomanagement Chancen und Herausforderungen bereitstellt.

13.2 Daten im Risikomanagement

13.2.1 Allgemeiner Überblick

Kern des betrieblichen Risikomanagements ist nach ISO 31000 die „koordinierte Aktivität zur Lenkung und Steuerung einer Organisation in Bezug auf Risiken“ (ISO Norm 31000:2018). Der Risikomanagement-Prozess sieht vor, die Risiken zunächst zu identifizieren, zu bewerten und in der Folge zu steuern, zu überwachen und darüber zu berichten. Eine wichtige Voraussetzung für ein erfolgreiches Risikomanagement ist daher eine laufende Überwachung, die auf die frühzeitige Erkennung von gefährdenden Entwicklungen abzielt. Hier spielen unterschiedliche Datenquellen für die Effektivität des Risikomanagements eine wichtige Rolle. In der Folge werden die Potenziale, die sich aus der Digitalisierung dieser Daten ergeben, einerseits auf die einzelnen Bestandteile des Risikomanagement-Prozesses projiziert und andererseits deren Auswirkungen auf die Zukunft der Unternehmenssteuerung abgeleitet.

13.2.2 Die wichtige Rolle von Daten im Risikomanagement-Prozess

13.2.2.1 Datenqualität

„You can't manage what you don't measure“ (McAfee et al. 2012, S. 64). Diese Aussage bringt nahe, dass messbare Informationen eine Grundvoraussetzung für ein erfolgreiches Risikomanagement sind. In diesem Zusammenhang spielt es in erster Linie keine Rolle, in welcher Form Daten analysiert werden. Durch die kritische Rolle des Risikomanagements für die Unternehmenssteuerung ergeben sich aber in der Konsequenz Anforderungen an die Datenqualität. Typische Dimensionen für die Datenqualität sind folgende (vgl. Otto und Österle 2016, S. 31):

- Korrektheit: Die sachliche Richtigkeit der Daten muss sichergestellt sein.
- Konsistenz: Falls es von einem Objekt mehrere Datenversionen geben sollte, müssen diese miteinander übereinstimmen.
- Vollständigkeit: Die Werte und Attribute eines Datensatzes sollen komplett vorhanden sein.
- Aktualität: Es muss sichergestellt sein, dass die Daten zu jedem Zeitpunkt mit dem aktuellen Status des realen Objektes übereinstimmen.
- Verfügbarkeit: Die Daten müssen zu jedem gewünschten Zeitpunkt für den Nutzer zugänglich sein.

Zu beachten ist, dass die Definition von Datenqualität kontextabhängig ist. Jeder Bestandteil des Gesamtprozesses beinhaltet eine Verarbeitung oder Erhebung spezifischer Informationen, die eine andere Datenqualität und unterschiedliche Datenquellen voraus-

setzen. Im Folgenden werden diese Anforderungen im Zusammenhang mit dem Risikomanagement-Prozess grob umrissen.

13.2.2.2 Risikoidentifikation

Für die Risikoidentifikation, die den ersten Schritt im Risikomanagement-Prozess darstellt, sind Daten ein unumgängliches Instrument zur Analyse. Das Risikomanagement-Modell der „Federation of European Risk Management Associations“ (FERMA) teilt die zu identifizierenden Risiken in die vier Kategorien „strategische Risiken“, „operationelle Risiken“, „finanzielle Risiken“ und „Gefahrenrisiken“ ein. Nach ISO 31000 werden folgende Methoden zur Identifikation vorgeschlagen:

- Historische Daten: Analyse von statistischen Daten aus Finanzberichten sowie organisatorische Abläufe in Form von Diagrammen.
- Theoretische Analysen: Szenario-Analysen strategischer Entscheidungen und Analysen bestehender Verträge mit Drittparteien wie Kunden, Versicherern und Zulieferern.
- Fachliche Stellungnahmen sowie Stakeholder-Bedürfnisse: Analyse der Unternehmensstrategie und Nutzung von unabhängigen Expertenmeinungen zur Feststellung von Risiken.

Betrachtet man potenzielle Datenquellen für die Risikoidentifikation, stößt man sowohl auf interne (Finanzberichte, interne Organisation, Verträge) als auch auf externe Ressourcen (Internetrecherche, Industriestandards, Marktforschung). Die Datenqualität ist für diesen Prozess in allen Ausprägungen entscheidend, da die Risikoidentifikation die Grundlage für den Gesamtprozess darstellt.

13.2.2.3 Risikobewertung, -aggregation & -steuerung

Die Risikobewertung folgt dem Prozess der Risikoidentifikation und sieht vor, die bereits identifizierten Risiken im Kontext ihres Ausmaßes zu bewerten. Die Vorgehensweisen hierzu werden in qualitative, semi-quantitative und quantitative Methoden unterteilt. Während Wettbewerbsanalysen wie die „Five-Forces“- oder „SWOT“-Analyse (vgl. Rohlf 2018, S. 109 ff.) qualitative Merkmale dokumentieren, werden einzelne, identifizierte Risiken (falls möglich) in einer Risikomatrix anhand von der Auftretenswahrscheinlichkeit und des Ausmaßes bewertet.

Die Bewertung dient dazu, das Vorgehen mit einem identifizierten Risiko zu bestimmen. Für das Risikomanagement ist die Richtigkeit der Einschätzung eines Risikos damit ein erfolgskritischer Faktor. Letztlich beruhen auch die zu Grunde liegenden Berechnungen auf einer Datenbasis, die für das Risikomanagement aufgebaut werden muss. Betrachtet man beispielsweise die Bewertung eines Naturkatastrophenrisikos, so liegt es nahe, hauptsächlich historische Daten aus externen Datenquellen zu nutzen, während auf der anderen Seite für neuartige Gefahren wie Cyber-Kriminalität oder die angesprochene Wettbewerbsanalyse eine andere Form der Datenbasis zur Bewertung eingesetzt werden muss (vgl. Wrede et al. 2018, S. 413 ff.). Die Diversifikation der Anforderungen spiegelt

sich auch in der Datenqualität wider, die sich je nach Quelle unterschiedlich zusammensetzt. Grundsätzlich gilt für die Genauigkeit des Prozesses jedoch, dass eine verbesserte Datenqualität auch einen verbesserten Prozess hervorbringt.

13.2.2.4 Risikokontrolle & -berichterstattung

Die Risikokontrolle und die Berichterstattung verlangen regelmäßige Dokumentationen und Berichterstattungen (vgl. Rohlfs 2018, S. 301 ff.). Zielsetzung ist die Beurteilung von Effizienz und Wirksamkeit des Risikomanagementprozesses. Diese Beurteilung sowie die Information über das Risikoprofil des Unternehmens haben entscheidende Auswirkungen auf die Unternehmenssteuerung. In diesem Zusammenhang spielen insbesondere die Datenrichtigkeit und Datenaktualität eine kritische Rolle für die Erreichung des genannten Ziels.

13.3 Digitale Daten als Effizienz- und Effektivitätstreiber

13.3.1 Vorteile digitaler Daten

Die Digitalisierung birgt die Möglichkeit, die Datenqualität an die Bedürfnisse des Risikomanagements anzupassen. Während im Rahmen der Vollständigkeit und Korrektheit keine Nachteile analoger Daten gegenüber digitalen Daten bestehen, können bei verantwortungsvoller Informationstechnologie im Unternehmen die Konsistenz, Aktualität und Verfügbarkeit durch digitale Daten gesteigert werden. Der Kern des Risikomanagements als „koordinierte Aktivität zur Lenkung und Steuerung einer Organisation in Bezug auf Risiken“ kann in seiner Effektivität durch diese erheblich positiv beeinflusst werden. Darüber hinaus wird die Datenerhebung für das Risikomanagement vereinfacht, sodass Mitarbeiter keine Feedback-Zyklen im eigenen Unternehmen durchlaufen müssen, um die Informationen zu erhalten, die sie benötigen. Ein weiterer Vorteil ist die globale Verfügbarkeit, Menge sowie Aktualität digitaler Daten. Ob Informationen zur Sicherheitslage, Unwetter- und Katastrophenmeldungen oder Finanzdaten zu eigenen Lieferanten, das Risikomanagement kann all diese Daten aus unterschiedlichen Quellen in digitaler Form sammeln und für Risikoidentifikation, -bewertung, -steuerung und -überwachung analysieren. Hierzu werden häufig sogenannte Application Programming Interfaces (API) angeboten, die bereits vorstrukturierte Daten meistens zu einem Entgelt über eine Internetschnittstelle zur Verfügung stellen.

Darüber hinaus können interne Schnittstellen eine Verknüpfung des Risikomanagements mit dem Controlling oder Rechnungswesen erzeugen und daraus folgend eine Echtzeit-Überwachung sogenannter Key Performance Indices (KPI) fördern, die die Leistung eines Unternehmens im aktuellen Zustand für einen bestimmten Bereich bewertet. Diese können zudem als Key Risk Indicators (KRI) genutzt werden, um die Risikoüberwachung und die -früherkennung in Echtzeit zu gewährleisten (vgl. Davies et al. 2006, S. 1 ff.).

Die Entwicklung hin zu einer Digitalisierung aller für das Risikomanagement notwendigen Datenquellen wird unterstützt von Konzepten wie Big Data, um das sich Methoden zur Speicherung und Verwaltung der großen, digitalisierten Datenmengen gebildet haben.

13.3.2 Big Data

Big Data wird häufig als Begriff für große Datenmengen verwendet (vgl. Chen et al. 2014, S. 171). Apache Hadoop (ein bekanntes Projekt im Rahmen der Verarbeitung großer Datenmengen) fasst im Jahr 2010 Big Data als Datensets zusammen, bei denen es nicht möglich ist, sie in einem akzeptablen Umfang zu erfassen, zu verwalten und zu verarbeiten (vgl. Chen et al. 2014, S. 173). Aus den vielen unterschiedlichen Arten der Beschreibung dieses Begriffes bilden sich vier in Englischer Sprache formulierte Charakteristika heraus, die diesen Begriff klarer beschreiben:

- Volume: Diese Eigenschaft geht auf die große Menge von Daten ein, die insbesondere in den letzten Jahren im Internet entstanden ist (vgl. McAfee et al. 2012, S. 64).
- Velocity: Dieser Begriff steht für die Geschwindigkeit der Datensammlung und der Zeitspanne, in der sie wertschöpfend sind (vgl. Fase 2014, S. 389).
- Variety: Big Data wird durch eine große Datenvielfalt mit unterschiedlichen Formaten und Quellen repräsentiert (vgl. McAfee et al. 2012, S. 65).
- Veracity: Dies bezieht sich auf die Vollständigkeit, Richtigkeit und Verlässlichkeit der Dateninhalte im Rahmen von Big Data (vgl. Dorschel 2015, S. 8).

13.3.3 Cloud Computing & Internet of Things (IoT)

Technologisch ist der Einsatz von Big Data Analysen einerseits von einer positiven Entwicklung des Cloud Computings unterstützt, das Unternehmen Rechenleistungen und Speicherfähigkeit zur Verfügung stellt (vgl. Avram 2014, S. 530 f.). In diesem Zusammenhang entsteht eine Wechselwirkung zwischen der Big Data-Nutzung und des Cloud Computings, bei denen eine Förderung der Datenmenge gleichzeitig die Nachfrage nach Speicher in der Cloud erhöht, durch die wiederum andere Unternehmen von einer erhöhten Preiseffizienz auf Basis der Kapazitätserweiterungen profitieren (vgl. Chen et al. 2014, S. 176). Zusätzlich zu diesem Begünstigungsverhältnis von Big Data und Cloud Computing kommt die technologische Unterstützung, die die werthaltige Nutzung von Big Data auch in der Cloud erst möglich macht. Beispielsweise schaffen es Hadoop-Ökosysteme Rechenleistungen und Speicherkapazitäten effizient zu verteilen, um die großen Datenmengen nicht nur speichern, sondern auch schnellstmöglich verarbeiten und auswerten zu können.

Zur Nutzung solcher Technologien können in einem Unternehmen Schnittstellen bis hin zu den kleinsten Prozessen ermöglicht werden, um die Daten daraus in einen gesamt-

unternehmerischen Kontext zu bringen. Treiber einer solchen Datengenerierung in der Industrie ist insbesondere IoT, das sich aus Geräten und Sensoren zusammensetzt, die gemeinsam im Netzwerk Daten sammeln und austauschen, um so die physische mit der digitalen Welt zusammenzubringen (vgl. Fleisch et al. 2015, S. 1). Die Daten, die sich aus einem solchen Netzwerk ergeben, sind auf der einen Seite interessant für automatisiert gesteuerte Produktion und bergen auf der anderen Seite Potenzial zur Risikoidentifikation, -bewertung und -überwachung sowie für ein angemessenes Frühwarnsystem. IoT liefert dem Risikomanagement damit große, heterogene Datenmengen, die in einem zeitlichen und örtlichen Spektrum identifiziert werden können, um eine Risikoanalyse zu ermöglichen.

13.4 Methoden zur Datenanalyse für das Risikomanagement

Demzufolge ist nach einer Studie des BARC Institutes der hauptsächliche Wert von Big Data nicht die große Menge Daten, sondern vordergründig die nahezu in Echtzeit bereitgestellten Analyseergebnisse (vgl. Bange und Janoschek 2014, S. 5). Hieran angeknüpft finden sich im Spektrum der Datenanalyse Begrifflichkeiten wie Business Intelligence (BI) und Predictive Analytics sowie künstliche Intelligenz wieder. Im Folgenden werden die Technologien voneinander abgegrenzt und die Vorteile aus der Datenanalyse für das Risikomanagement dargestellt.

13.4.1 Überblick

Abb. 13.1 gibt Aufschluss über die Anordnung der analytischen Methoden zur Datenanalyse, die zusammenfassend als Analytics bezeichnet wird.

Big Data Analytics vermag die Auswertung der großen Datenmengen im Rahmen der Datensphäre Big Data zu beherrschen (vgl. Leveling et al. 2014, S. 1). Die Abgrenzung von Big Data Analytics zu den klassischen Analytics-Methoden ist der strenge Bezug zu den Charakteristika, die zuvor beschrieben wurden. Business Intelligence (BI), das durchaus in Kombination mit Big Data funktionieren kann, ermöglicht eine Aufnahme eines vergangenen Zustandes durch sinnhaftes Zusammenfügen und Abbilden (vgl. Jacobi und Groher 2019, S. 548 f.). Das Ziel von BI ist die Nachvollziehbarkeit aktueller Zustände im Unternehmen auf Basis vergangener Informationen. Die begriffliche Einordnung von BI beschränkt dabei nicht die Art der Datengewinnung bezüglich Anzahl, Lokalisierung und Art der Datenquellen sowie deren Einsatzzweck (vgl. Dittmar 2016, S. 57).

Als Teilbereich von BI verfolgt Business Analytics den Ansatz, unternehmerische Entscheidungen durch Erkenntnisse aus verfügbaren Daten zu unterstützen (vgl. Chamoni und Gluchowski 2017, S. 9). Daraus entstehende Datenanalysemethoden hingegen beinhalten diejenigen Methoden, die sich von den klassischen Verfahren insofern abgrenzen, als dass sie neuartige Technologien wie neuronale Netze, Zeitreihenanalysen und weitere

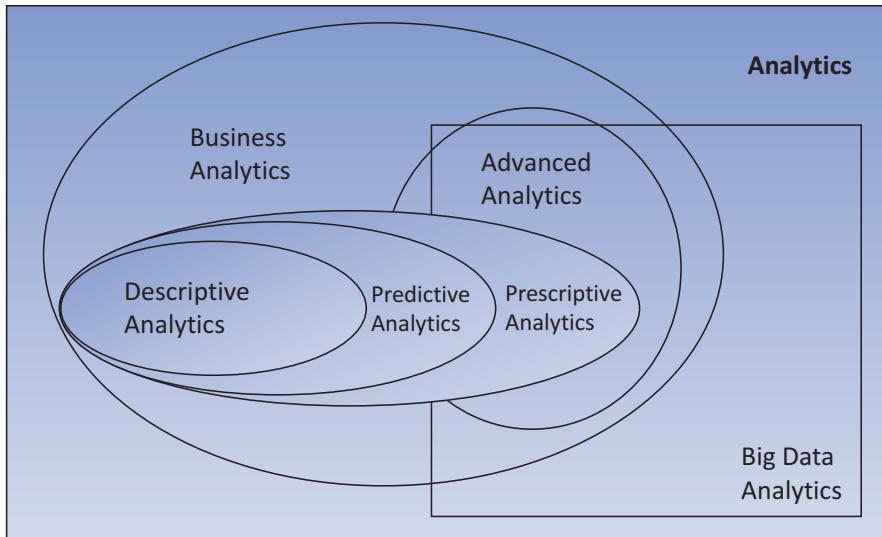


Abb. 13.1 Übersicht für Data Analytics. (Quelle: eigene Darstellung in Anlehnung an Gluchowski 2016, S. 277)

Lernverfahren nutzen, um aus vorhandenen Daten einerseits Prognosemodelle (Predictive Analytics) und andererseits Kausalanalysen sowie Handlungsempfehlungen für die Zukunft (Advanced & Prescriptive Analytics) ableiten zu können (vgl. Chamoni und Gluchowski 2017, S. 9 ff.).

13.4.2 Nutzen für das Risikomanagement

Die sich ergebenen Vorteile aus der Datenanalyse für das Risikomanagement sind vielfältig, denn sie erstrecken sich damit nicht nur über die reine Datenbeschaffung, sondern gehen so weit, dass der gesamte Risikomanagement-Prozess in Echtzeit ablaufen kann. Für die Unternehmenssteuerung und das Risikomanagement kann sich somit ein Paradigmenwechsel von „reakтив analytisch zu proaktiv prognostizierend“ (vgl. Kieninger et al. 2015, S. 5) vollziehen. Betrachtet man die Möglichkeit, Prognosemodelle aus bestehenden Daten zu entwickeln, so kann das Risikomanagement von einer ganz neuen Form der Risikoüberwachung profitieren.

Predictive Maintenance (zugehörig dem Thema Predictive Analytics) ist eine solche Analysemethode, die sich der Idee annimmt, proaktives Risikomanagement in der Industrie zu ermöglichen. Dabei fokussiert sich dieser Ansatz darauf, Maschinenausfälle vorherzusagen, um somit die zustandsbasierte mit der vorausschauenden Wartung abzulösen. Im Kontext von Industrie 4.0 sollen damit die Ablauf- und Instandhaltungsplanung verzahnt werden (vgl. Zhai und Reinhart 2018, S. 298). Voraussetzung für den Einsatz dieser Strategie ist die Nutzung echtzeitfähiger, kommunizierender Systeme, deren Datenströme durch intelligente Algorithmen das Verschleißverhalten der genutzten Maschine analysie-

ren (vgl. Zhai und Reinhart 2018, S. 299). Als weiteres Beispiel für Predictive Analysis kann eine Umsatzprognose die Beeinflussung der KRIs für die Zukunft simulieren (vgl. Möller et al. 2016, S. 1 ff.). Eine Implementierung solcher Konzepte in den Risikomanagement-Prozess bestärkt den bereits angesprochenen, proaktiven Ansatz und die Verwendung digitaler Daten im Kontext der Unternehmenssteuerung. Sowohl der Bereich der Risikoüberwachung, als auch ein angemessenes Risikofrühwarnsystem können auf Basis trainierter, prädiktiver Modelle erheblich effektiver gemacht werden.

Über das Konzept des prädiktiven Risikomanagements hinaus kommt hinzu, dass durch ein Echtzeit-Reporting Entscheidungen gestützt werden, für die der Einfluss aufgezeichneter Kennzahlen benötigt wird. Horváth und Michel beschreiben es in ihren zehn Thesen zur Veränderung der Unternehmenssteuerung als „agile real-time“ Steuerungszyklen, die zunehmend auf automatisierten und funktionsübergreifenden Abhängigkeiten und Zusammenhängen basieren (vgl. Kieninger et al. 2015, S. 6). Diese Treiber schneller Managemententscheidungen sorgen für eine andere Art der Berichterstattung. Während laut der Studie von Horváth & Partner lediglich sechs von 20 Unternehmen eine monatliche Berichterstattung der „Top-Risiken“ vornehmen, tendieren die Meinungen der befragten Experten dahin, dass sich diese Frequenz erhöhen wird, sodass mindestens acht der Befragten in Zukunft monatlich berichten werden (vgl. Hopfener et al. 2018, S. 30).

Inkonsistent mit dem Gesamteindruck über die Wichtigkeit digitaler Daten und deren Auswertung, verwenden nur 25 Prozent der Unternehmen, denen die Experten angehören, tatsächlich Technologien wie Predictive Analysis und Big Data, während 92 Prozent der Befragten einer Studie von Horváth & Partner der Anwendung dieser Methoden eine wichtige bis sehr wichtige Rolle beimessen (vgl. Hopfener et al. 2018, S. 24). Im Zuge der Digitalisierung erhöhen sich die Chancen, diese Technologien einsetzbar zu machen, andererseits besteht im Gegenzug die Gefahr bei Nichtnutzung oder Nutzung ineffizienter Technologie, Wettbewerbsvorteile zu verlieren.

13.5 Herausforderungen aus der Digitalisierung

13.5.1 Einleitung

Für die Nutzung der Vorteile aus der treibenden Idee des proaktiven Risikomanagements ergeben sich organisatorische Maßnahmen, die es unternehmensweit zu beachten gilt. So entstehen sowohl Anforderungen an neue Kompetenzen für den Umgang mit digitalen Daten, als auch neue Arten von Risiken und damit verknüpfte Maßnahmen, die in den Verantwortungsbereich des Risikomanagements fallen.

13.5.1.1 Data Science als neue Kompetenz des Risikomanagements

Notwendigkeit einer neuen Kompetenz

Es wurde bereits eine Einführung in das Thema Datenqualität gegeben. Sowohl für den eigenen Risikomanagement-Prozess als auch für andere Bereiche im Unternehmen ist die Gewährleistung der Datenqualität ein sehr wichtiges Thema.

Bezüglich der Datenverfügbarkeit besteht aufgrund wachsender Datenmengen die Herausforderung, einen Mechanismus zu finden, den Datenzugriff, die Datenbereinigung sowie deren Integration mit entsprechender Vollständigkeit und Korrektheit in einem vertretbaren Zeitrahmen zu ermöglichen (vgl. Cai und Zhu 2015, S. 3). Zudem besteht die Gefahr, die Aktualität nicht immer gewährleisten zu können. Die Analysemöglichkeiten von Echtzeitdaten für ein Unternehmen erhöhen die Anforderungen an die Prozessierung, denn sie verringern die Veränderungszyklen der Daten (vgl. Cai und Zhu 2015, S. 3).

Betrachtet man den beschriebenen Zugang zu Echtzeit-Daten im Rahmen von IoT, die Hinzuziehung eigener Finanzdaten im Unternehmen sowie Informationen zu Wettbewerbern und Kunden aus dem Internet, so entstehen darüber hinaus eine Vielzahl an Datentypen und -strukturen, mit denen es sich auseinanderzusetzen gilt (vgl. Cai und Zhu 2015, S. 3). Gerade im Zuge der Digitalisierung, in der die Unternehmen die Datenqualität nicht mehr als „Hygienefaktor“ wahrnehmen, sondern als kritisch für den operationellen Erfolg betrachten (vgl. Otto und Österle 2016, S. 11), wird vom Risikomanagement eine Kompetenz für den Umgang mit Daten erwartet.

Während die Nutzung neuester Analysetools sowie deren Auswahl bereits Knowhow voraussetzt, können sich durch langfristige Veränderungen in diesem Umfeld ganz neue Anforderungen an die Mitarbeiter des Risikomanagements ergeben. Da die korrekte Nutzung digitaler Daten als Prognosehilfe in einem Szenario der automatischen Datenanalyse eine enorme Wichtigkeit hat, erhöht sich die Notwendigkeit, eine eigene Kompetenz in diesem Bereich aufzubauen und mit Mitarbeitern zu besetzen, die einerseits die fachliche Kompetenz und andererseits das technische Knowhow für diese neuen Aufgaben mitbringen. Zukünftig sollten BI, Predictive Analytics oder Machine Learning keine Fremdwörter im Jargon des Risikomanagements sein, denn sie können im Rahmen einer automatisierten Analyse über die Funktionsfähigkeit der Organisation entscheiden.

Die sich ergebenen Vorteile aus diesen neuen Möglichkeiten werden durch eine Verlagerung der Kapazitäten begleitet, sodass der Fokus sich von manueller hin zu automatisierter Recherche und Auswertung verschiebt und damit Zeit für analytische und strategische Aufgaben des Risikomanagers schafft. Damit entsteht mehr Raum für Entscheidungen für den Risikomanager und im Umkehrschluss auch neue Anforderungen an dessen Qualifikationen (vgl. Schröder et al. 2019, S. 133).

Data Scientist als neues Berufsbild

Für die Erfüllung dieser Anforderungen erfreut sich ein für das Risikomanagement neues Berufsbild besonderer Attraktivität. Der mit „Data Scientist“ eingedeutschte Begriff kombiniert Methodenkenntnisse, die insbesondere die genannten Machine-Learning-, Predictive-Analytics- aber auch klassische Mathematik- und Statistikfähigkeiten betrifft, mit technischen Kompetenzen, die die darunterliegende Datenverarbeitungsschicht wie Datenbankensysteme, Rechnerarchitekturen oder Cloud-Umgebungen abdecken (vgl. Markl et al. 2013, S. 3). Hierbei zeichnen sich gute Data Scientists dadurch aus, den Kontext der Analysen fachlich nachvollziehen und methodisch lösen zu können, um den größten Mehrwert für die Organisation zu schaffen. Auf der anderen Seite müssen sie aber auch

deren Ergebnisse und die daraus folgenden Lösungen in einer Weise vortragen, dass sie das Top-Management anspricht. „Der Idealtypus des Data Scientists ist Forscher, Entwickler, Marketing-Spezialist und Verkäufer in einer Person“ (Steiner und Welker 2016, S. 70).

Die Erwartungshaltung an einen solchen Beruf verspricht einerseits eine besonders fundierte theoretische und praktische Ausbildung, andererseits müssen für die Beschäftigung qualifizierter Fachkräfte, die einen Mehrwert für das Unternehmen generieren können, betriebswirtschaftlich hohe Kosten eingeplant werden.

Make or Buy

Klassische Methoden wie die Nutzung von Microsoft Excel werden in einem Szenario der automatisierten Datenanalyse langfristig kaum genutzt. Cloud-Plattformen bieten auf der einen Seite bereits effiziente Verarbeitungsmethoden für große Datenmengen, auf der anderen Seite können diese Anbieter durch eigene Kompetenzen im Bereich Data Science, Tools zur Verfügung stellen, die die Fähigkeiten eines Data Scientists zumindest teilweise konsolidieren. Im Falle einer Nutzung solcher Lösungen, fallen die technische Implementierung und der Aufbau der Datenquellen und Infrastruktur nicht mehr auf den Data Scientist zurück. Dennoch wird eine Kompetenz benötigt, die einen fachlichen Sinn der verfügbaren Daten für das Risikomanagement herstellt.

Der Königsweg könnte sein, eine Kombination hochwertiger Analysetools und eine Handvoll bestmöglich qualifizierter Fachkräfte für den Bereich Data Science einzusetzen, um somit von den Vorteilen des technologischen Wandels über die Cloud-Plattformen zu profitieren und die Verknüpfung eigenen fachlichen Knowhows mit den technischen Anforderungen langfristig zu vereinen. Diese grundlegende Entscheidung obliegt letztlich dem Management des jeweiligen Unternehmens.

13.6 Neue organisatorische Aufgaben durch digitale Daten

13.6.1 Data Governance

Corporate Governance ist ein wichtiger Begriff im Rahmen der Unternehmensführung und auch des Risikomanagements. Es umfasst den Ordnungs- und Handlungsrahmen, in dem das Unternehmensmanagement Entscheidungen trifft und umsetzt. Die in dem Unternehmen anfallenden Prozesse, Vermögenswerte sowie dessen Ressourcen fallen wiederum unter die Aufsicht der Corporate Governance (vgl. Brüning et al. 2017, S. 4). Da die Daten eines Unternehmens einen Schlüssel-Vermögenswert darstellen, ist es eine Verpflichtung, eine IT-Governance zu definieren, die für das Management der IT verantwortlich ist (vgl. Weill und Ross 2004, S. 1 ff.). Abgegrenzt von der IT-Governance, deren hauptsächliche Aufgabe darin besteht, eine möglichst wirtschaftliche Gestaltung von IT-Systemen zu bewirken, widmet sich die Data Governance den (digitalen) Daten und Informationen (vgl. Brüning et al. 2017, S. 4). Mit dem Ziel, den Nutzen aus der Verwendung von Daten zu



Abb. 13.2 Komponenten von Data Governance. (Quelle: eigene Darstellung in Anlehnung an Brüning et al. 2017, S. 7)

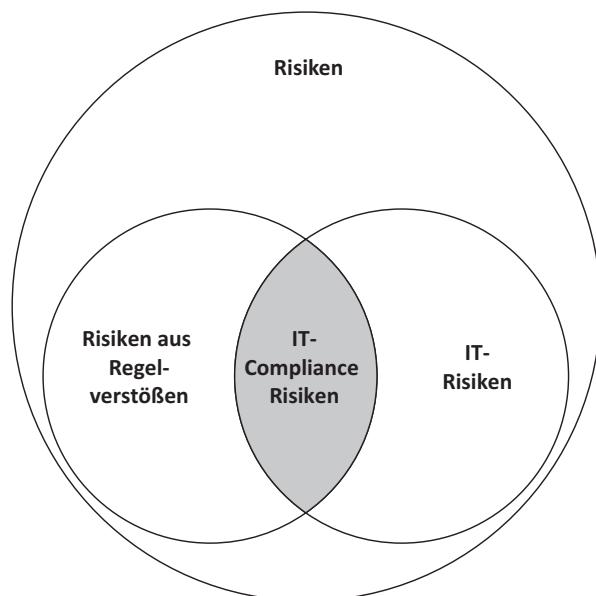
maximieren, umfasst Data Governance alle Führungsaufgaben zu organisatorischen Maßnahmen, Richtlinien sowie Prinzipien, die mit dem risikofreien Zugang zu korrekten Daten zusammenhängen (vgl. Abb. 13.2).

Die Data Management Association (DAMA) hat unter der Bezeichnung DAMA-Data Management Body of Knowledge ein Konzept erstellt, in dem Data Governance als Mittelpunkt für elf Komponenten den Ankerbaustein bildet (vgl. Brüning et al. 2017, S. 6). Damit greift Data Governance einige der bereits hier behandelten Themen auf und verspricht dem Gesamtunternehmen und Risikomanagement qualitativ hochwertige Daten für eine effiziente Unternehmenssteuerung.

13.6.2 IT-Compliance

Vor allem das Thema Compliance ist durch neue gesetzliche Regelungen für Unternehmen unterschiedlicher Branchen verschärft worden. Die im Zuge der Datenschutzgrundverordnung (DSGVO) verschärften Bestimmungen erfordern eine klare Abgrenzung in Bezug auf die Behandlung personenbezogener Daten. Zum einen wird für diese eine Einwilligung für die Speicherung und Nutzung gefordert, zum anderen bestehen Auskunfts- und Löschungspflichten. Darüber hinaus kommen Pflichten zur Dokumentation von Verarbeitungstätigkeiten und zum Nachweis von Schutzmaßnahmen personenbezogener Daten hinzu. Der Hintergrund für die Veröffentlichung dieses rechtlichen Rahmens für die gesamte EU ist ein Schutz der „Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten“ (Art. 1 Abs. 2 DSGVO). Hieraus ergibt sich für alle Unternehmen, die mit Daten von EU-Bürgern arbeiten, ein kontinuierlicher Prozess, der im Rahmen der Unternehmenssteuerung integriert werden muss. Eine wichtige Bedeutung wird damit dem Thema IT-Compliance beigemessen, das Risiken adressiert, die durch Fehlfunktionen der IT entstehen. Zum Aufgabenbereich gehört ebenfalls eine schlechte Organisation in Form eines unzureichenden Betriebes, der Nutzung sowie der Verfügbarkeit und der Sicherung zu verhindern, um die gesetzlichen Auflagen jederzeit erfüllen zu können (vgl. Klotz und Dorn 2008, S. 6). Die Anforderungen der neuen Datenschutz-Verordnung sind somit eng verzahnt mit den Aufgaben des Risikomanagements (vgl. Abb. 13.3).

Abb. 13.3 Einordnung von Risiken. (Quelle: eigene Darstellung in Anlehnung an Klotz und Dorn 2008, S. 7)



13.6.3 Organisatorisches Daten-Management

Eine andere Schnittstelle für das Risikomanagement ergibt sich aus dem Potenzial von Daten als unternehmerische Ressource im Zusammenhang mit den Analyseverfahren, die bereits in Abschn. 13.2 erörtert wurden. Hieraus entstehen insbesondere Anforderungen an die Datenqualität, denn das Risikomanagement ist in einem solchen Szenario abhängig von konsistenten, korrekten und aktuellen Daten. Die Beschaffung dieser Daten ist in erster Linie von einer interdisziplinären Zusammenarbeit abhängig. Das liegt hauptsächlich an sogenannten „Datensilos“, die den Austausch und die Analyse über Abteilungsgrenzen hinaus erschweren (vgl. Brockmann 2018, S. 638). Auch die Qualität der Daten in unterschiedlichen Bereichen der Organisation kann zu Lasten der Verarbeitungseffizienz sehr stark variieren. Wenn die Organisation in einer Form aufgebaut ist, dass eine Vernetzung der Bereiche stattfindet und technologisch verknüpft ist und damit die Voraussetzungen für eine gemeinsame Datenbasis entstehen, wird das Risikomanagement durch eine Echtzeit-Risikoüberwachung unterstützt und das gesamte Unternehmen kann von den Auswertungsergebnissen profitieren (vgl. Schröder et al. 2019, S. 33). Gerade die Verfügbarkeit im Rahmen der Datenqualität kann von einer solchen Zusammenarbeit erheblich begünstigt werden. Ein Vorteil in diesem Bereich ist insbesondere die Nutzung passender Technologie und Software, die die Unternehmensbereiche adäquat miteinander verbindet. In diesem Zusammenhang können prozesseitig sogenannte Enterprise-Resource-Planning(ERP)-Systeme Abhilfe schaffen (vgl. Jacob 2008, S. 1 ff.). Auf Ebene der Datenverwaltung können Data-Warehouse- und Big-Data-Technologien Voraussetzungen für funktionierende BI und BA darstellen.

13.7 Neuartige Risiken aus der Digitalisierung

13.7.1 Cyber-Risiko

Eine Studie von Deloitte aus dem Jahr 2017 stellt fest, dass 93 Prozent der Unternehmen dem Thema IT-Sicherheit mindestens einen „hohen“ Stellenwert zusprechen (vgl. Deloitte GmbH 2017, S. 9). Das hiermit in Verbindung stehende Risiko wird mit dem Begriff „Cyber“ assoziiert, der sich aus der Kybernetik ableitet und oft im Zusammenhang künstlicher Realitäten verwendet wird. Somit werden Datenräume digitaler Netze und IT-Systeme von Unternehmen in den Wirkungsbereich von Cyber miteingeschlossen (vgl. Biener et al. 2015, S. 4). Die Risiken zählen grundsätzlich zu den operationellen Unternehmensrisiken (vgl. Haas und Hofmann 2013, S. 10) und beinhalten darüber hinaus das Thema „Reputationsrisiko“, welches eine große Bedeutung in diesem Kontext hat (vgl. Biener et al. 2015 S. 7). Das Cyber-Risiko, dessen Auswirkungen sich beispielsweise in Identitätsdiebstahl, Weitergabe sensibler Daten oder Betriebsunterbrechung äußert, kann Ursachen wie höhere Gewalt, menschliches sowie technisches Versagen haben, ist aber auch auf kriminelle Aktionen wie Hackerangriffe, physische Angriffe oder Erpressungen zurückzuführen.

Durch die Digitalisierung entwickelt sich eine immer größer werdende Angriffsfläche im Zusammenhang mit Cyber-Risiken.

Unternehmen sind auf Basis informationstechnischer Anforderungen wie Speicherkapazitäten und Skalierbarkeit vermehrt dazu gezwungen, eigene Ressourcen auszubauen, entsprechend nachzurüsten oder sich externen Anbietern und insbesondere Cloud-Dienstleistern zu bedienen (vgl. Haas und Hofmann 2013, S. 1). Die hieraus entstehenden Cyber-Risiken sind unterschiedlich ausgeprägt. Während eine Softwarenutzung als Software-as-a-Service (SaaS) in der Cloud insbesondere eine Exponierung der eigenen Daten zur Folge hat, besteht bei der Nutzung reiner IT-Ressourcen über Platform-as-a-Service (PaaS) oder einer bestehenden Infrastruktur als Infrastructure-as-a-Service (IaaS) auf Cloud-Basis eine Abhängigkeit in der Sicherung eigener Daten von dem Anbieter des Dienstes. Das kann im Rahmen der Gesamtwirtschaft zu weltweiten Kumulproblemen führen (vgl. Haas und Hofmann 2013, S. 10) und auf Unternehmensebene nicht vorhersehbare Folgen haben.

Zusätzlich erhöhen sich durch die zunehmende Vernetzung der Produktion in der Industrie die Cyber-Risiken exponentiell. Durch den Aufbau autonom handelnder Systeme, die mithilfe von Vernetzung gesteuert werden, entstehen hohe Risiken durch Angriffe auf die Hardware sowie Verletzlichkeiten im Gesamtnetzwerk. Cyber-Angrifer, die in dieses Netzwerk gelangen, haben potenziell Zugriff auf Steuerungssysteme und können diese sabotieren (vgl. Hertel 2015, S. 725). Hinzu kommen menschliches Versagen und technische Fehlfunktionen als weitere Risikofaktoren, die Auswirkungen auf die Gesamtproduktivität des Unternehmens haben können.

13.7.2 Geschwindigkeit technologischer Fortschritte

Wie bereits dargestellt, entwickeln sich die vorhandenen Datenmengen in Größen, die kaum noch zu fassen sind (vgl. Cisco Systems 2018). Diese Entwicklung wird auf der einen Seite durch die zunehmende Digitalisierung der Gesellschaft gefördert und auf der anderen Seite durch die Vernetzung der Produktion, die Steigerung der Rechenleistungen oder die Nutzung von Big-Data-Technologien begünstigt. Darüber hinaus definiert sich die Digitalisierung nicht nur durch Datenmengen und Rechenleistung, sondern auch durch Technologien, die sich derer Inhalte bedienen. Als Beispiele können hier autonomes Fahren, künstliche Intelligenz oder Blockchain genannt werden, die das Potenzial zu einer Veränderung der organisatorischen Abläufe in einem Unternehmen haben.

Betrachtet man in diesem Zusammenhang die Rolle des Risikomanagements, das als „koordinierte Aktivität zur Lenkung und Steuerung einer Organisation in Bezug auf Risiken“ (ISO Norm 31000:2018) fungiert, muss die Tätigkeit an diese Entwicklungen angepasst werden, damit eine angemessene Risikoidentifizierung und -bewertung stattfinden kann. Besonders im Rahmen der Nutzung dieser neuen Technologien, bedarf es über die beschriebenen neuen Kompetenzen hinaus, reaktionsschnelle Risikobewertungsmethoden, die die möglichen Konsequenzen eines Einsatzes neuer Technologien einschätzen können.

13.8 Fazit

Digitale Daten stellen für den Risikomanagementprozess den entscheidenden Vorteil dar, die Datenqualität erheblich steigern zu können. Die schnelle Verfügbarkeit, die Konsistenz und insbesondere die Aktualität von Daten können den Risikomanagement-Prozess in seiner Effizienz und Effektivität verbessern. Hierbei bestehen für die Analyse und Prognostizierbarkeit von Daten sowie der Echtzeit-Berichterstattung einige Anknüpfungspunkte der Digitalisierung, Veränderungen für den Prozess hervorzurufen. Gerade im Rahmen der Identifikation und Bewertung von Risiken können Schnittstellen für digitale Daten entstehen, die den Gesamtprozess effektiver machen. Durch Leistungs- und Risikoindikatoren, die durch die Digitalisierung in Echtzeit verfügbar gemacht werden können, entstehen neue Möglichkeiten für automatisierte Frühwarnsysteme, die latente Bedrohungen mit zeitlichem Vorlauf zu erkennen vermögen (vgl. Krystek 2007, S. 355).

Im Kontext der Unternehmenssteuerung ermöglichen Big Data-Technologien Echtzeit-Reportings, die Management-Entscheidungen in Echtzeit unterstützen und langfristig möglicherweise automatisieren lassen. Hier birgt die Digitalisierung die Chance zu einem Paradigmenwechsel von einem „reakтив analytischen“ hin zu „proaktiv prognostizierenden“ Risikomanagement (vgl. Kieninger et al. 2015, S. 5). Diese Auswirkungen auf die Unternehmenssteuerung, zu denen das Risikomanagement maßgeblich beitragen kann, bergen erhebliche Effizienz- und Effektivitätssteigerungspotenziale, die es aus Sicht der Unternehmen zu nutzen gilt. Zeitlich gesehen werden einige Prognosen bezüglich des Einsatzes besprochener Technologien im Risikomanagement diskutiert. Einer Experten-Umfrage zu Folge, ist von einem Fünf- bis Zehnjahreshorizont bezüglich der Umsetzung von Automatisierung, Big Data und Vernetzung von Daten auszugehen (vgl. Hopfener et al. 2018, S. 36).

Neben den beschriebenen Vorteilen ergeben sich für das Risikomanagement auch Herausforderungen durch die fortschreitende Digitalisierung. Durch die steigenden Anforderungen an den Umgang mit Daten, hat das neue Berufsbild des Data Scientist das Potenzial, ein wichtiger Baustein des Risikomanagements zu werden. Zu den neuen Fachkompetenzen kommen Anforderungen an den Umgang mit Daten, die das Risikomanagement mitverantwortet. Data Governance sowie IT-Compliance sind wichtige Themenkomplexe, mit denen es sich auseinanderzusetzen gilt.

Um die gesamten Potenziale der Datenanalyse auszuschöpfen, ist es notwendig, die Organisation und die dazugehörigen Prozesse digital miteinander zu verknüpfen. Zwar wird das Risikomanagement auf die technische Umsetzung wohl keinen direkten Einfluss haben, die daraus folgenden Vorteile der Überwachung der Prozesse im Gesamtunternehmen sind für das Risikomanagement jedoch nahezu grenzenlos.

Über diese organisatorischen Herausforderungen hinaus, birgt die Digitalisierung neuartige Risiken, mit denen das Risikomanagement umzugehen hat. Das ständig wachsende Cyber-Risiko und die Anforderungen an den Umgang mit der zunehmenden Geschwindigkeit des digitalen Wandels, lassen darauf schließen, dass sich das Risikomanagement in

Zukunft weitere Kompetenzen aneignen muss, um seiner Kernaufgabe, der „Lenkung und Steuerung einer Organisation in Bezug auf Risiken“ (DIN 2018, S. 7), weiterhin adäquat nachkommen zu können.

Literatur

- Avram, M. (2014). Advantages and challenges of adopting cloud computing from an enterprise perspective. *Procedia Technology*, 12, 529–534. https://www.sciencedirect.com/science/article/pii/S221201731300710X/pdf?md5=a97ea31597bfb5b9bffa5c2b430a5b16&pid=1-s2.0-S221201731300710X-main.pdf_&_valck=1. Zugegriffen am 27.05.2019.
- Bange, C., & Janoschek, N. (2014). *Big data analytics 2014 – Towards a data-driven economy*. BARC Institute. <http://barc-research.com/wp-content/uploads/2014/06/BARC-big-data-analytics-2014-EN.pdf>. Zugegriffen am 06.05.2019.
- Biener, C., Eling, M., Matt, A., & Wirsfs, J. H. (2015). *Cyber risk: Risikomanagement und Versicherbarkeit* (S. 114). Institut für Versicherungswirtschaft der Universität St. Gallen. https://www.kessler.ch/fileadmin/user_upload/Cyber_Risk_Risikomanagement_und_Versicherbarkeit_de.pdf. Zugegriffen am 04.04.2019.
- Bitkom. (2019). Welches sind die wichtigsten IT-Trends des Jahres 2018? *Statista – Das Statistik-Portal*. <https://de.statista.com/statistik/daten/studie/808775/umfrage/die-wichtigsten-trends-in-der-itk-branche/>. Zugegriffen am 26.04.2019.
- Brockmann, H. C. (2018). Effizientes und verantwortungsvolles Datenmanagement im Zeitalter der DSGVO. *Datenschutz und Datensicherheit-DuD*, 42(10), 634–639. https://idp.springer.com/authorize/casa?redirect_uri=https://link.springer.com/content/pdf/10.1007/s11623-018-1015-0.pdf&casa_token=bFcm0QDyi_kAAAAA:wSJefZxPe5pTeNYjPU9-gZSdsLY1MPr8m3vBfBF9HNIVn9Nz4YQKHMz8fGXkA3ZRKM5d5n3TjErD-lvl. Zugegriffen am 24.06.2019.
- Brüning, A., Gluchowski, P., & Kaiser, A. (2017). Data Governance–Einordnung, Konzepte und aktuelle Herausforderungen (No. 015). *Chemnitz Economic Papers*. <https://www.econstor.eu/bitstream/10419/170675/1/CEP015.pdf>. Zugegriffen am 17.05.2019.
- Cai, L., Zhu, Y. (2015). The challenges of data quality and data quality assessment in the big data era. *Data Science Journal*, 14, 2. <https://doi.org/10.5334/dsj-2015-002>. Zugegriffen am 08.05.2019.
- Chamoni, P., & Gluchowski, P. (2017). Business analytics – State of the art. *Controlling & Management Review*, 61(4), 8–17. https://idp.springer.com/authorize/casa?redirect_uri=https://link.springer.com/article/10.1007/s12176-017-0030-6&casa_token=xvM99GP2NtAAAAAA:_us-J2EQJB3H_r_nQMojG2oLh3gvkI7L2aQrHIZvDWCeQRijyFFygob8hSSbdpvaJfJcD4sNm-cg72QxY. Zugegriffen am 01.05.2019.
- Chen, M., Mao, S., & Liu, Y. (2014). Big data: A survey. *Mobile Networks and Applications*, 19(2), 171–209. https://idp.springer.com/authorize/casa?redirect_uri=https://link.springer.com/article/10.1007/s11036-013-0489-0&casa_token=GLqS1aWqt30AAAAAA:jHYvO6hW-sfnhOw62n-QbhCKIYyrxjqJOjt-sTU1fQuz_ZS4ck1xhsYCcaNuD-vD8Zge4KAuwA4OgC8. Zugegriffen am 26.05.2019.
- Cisco Systems n.d. (2018). Prognose zum Volumen der gespeicherten Datenmenge in Rechenzentren weltweit in den Jahren 2016 bis 2021 (in Exabyte). *Statista – Das Statistik-Portal*. <https://de.statista.com/statistik/daten/studie/819487/umfrage/prognose-zum-weltweit-gespeicherten-datenvolu-men-in-rechenzentren/>. Zugegriffen am 03.06.2019.
- Davies, J., Finlay, M., McLenaghan, T., & Wilson, D. (2006). *Key risk indicators – their role in operational risk management and measurement* (S. 1–32). Prague: ARM and RiskBusiness Inter-

- national. <https://pdfs.semanticscholar.org/09b3/37587bd369b540157abee7e88f828798908f.pdf>. Zugegriffen am 07.04.2019.
- Deloitte GmbH. (2017). Cyber-security report 2017 – Teil 2: Cyber-Risiken in Unternehmen. <https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/RA-Risk-Advisory-Cybersecurity-Report-2017-2-14122017-s.pdf>. Zugegriffen am 01.07.2019.
- Dewenter, R., & Lüth, H. (2016). Big data aus wettbewerblicher Sicht. *Wirtschaftsdienst*, 96(9), 648–654. https://idp.springer.com/authorize/casa?redirect_uri=https://link.springer.com/content/pdf/10.1007/s10273-016-2029-6.pdf&casa_token=MDYIkFXGJfkAAAAA:vXNKseEBSksPs-MNnyEaYBzq3mMUdx1YfMBRCAgWQ_Zmi9AbG5FO-ikM4UoqAj81jVEBMPyYWvxqs-Row. Zugegriffen am 04.05.2019.
- DIN Deutsches Institut für Normung e. V. (2018). *Risikomanagement – Leitlinien* (ISO 31000:2018). Berlin: Beuth.
- Dittmar, C. (2016). Die nächste Evolutionsstufe von AIS: Big Data. In *Analytische Informationssysteme* (S. 55–65). Springer Gabler. http://emea.nntdata.com/uploads/tx_datamintsnodes/1603_DE_ARTICLE_BIG_DATA_Analytische_Informationssysteme.pdf. Zugegriffen am 20.05.2019.
- Dorschel, J. (2015). *Praxishandbuch Big Data. Wirtschaft-Recht-Technik*. Gabler, Wiesbaden (SpringerLink: Bücher). <https://www.nomos-elibrary.de/10.5771/978345263205-232/industrie-4-0-und-big-data-wirklich-ein-neuer-technologieshub>. Zugegriffen am 23.05.2019.
- Ernst & Young GmbH. (2019). *Start-up-Barometer Deutschland*. [www.ey.com, https://www.ey.com/Publication/vwLUAssets/ey-start-up-barometer-deutschland-januar-2019/\\$FILE/ey-start-up-barometer-deutschland-januar-2019.pdf](http://www.ey.com, https://www.ey.com/Publication/vwLUAssets/ey-start-up-barometer-deutschland-januar-2019/$FILE/ey-start-up-barometer-deutschland-januar-2019.pdf). Zugegriffen am 14.05.2019.
- Fase, D. (2014). Big Data—Eine Einführung. *HMD Praxis der Wirtschaftsinformatik*, 51(4), 386–400. https://idp.springer.com/authorize/casa?redirect_uri=https://link.springer.com/article/10.1365/s40702-014-0054-8&casa_token=1qARNn4nGmEAAAAA:3nIz8lJ5EY1Jf-2w17MWnk-WKXSLcdRhEOOefCd0a_gE4vsawORwcK0P2GOhDh-jnt0xdmZ-Jov0Zo. Zugegriffen am 11.04.2019.
- Fleisch, E., Weinberger, M., & Wortmann, F. (2015). Geschäftsmodelle im internet der dinge. *Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung*, 67(4), 444–465. <https://link.springer.com/content/pdf/10.1007/BF03373027.pdf>. Zugegriffen am 13.05.2019.
- Ganschar, O., Gerlach, S., Hämerle, M., Krause, T., & Schlund, S. (2013). Produktionsarbeit der Zukunft-Industrie 4.0 (Bd. 150). In D. Spath (Hrsg.). Stuttgart: Fraunhofer Verlag. http://www.mechatronik-bw.de/attachments/article/272/Fraunhofer-IAO-Studie_Produktionsarbeit_der_Zukunft_-Industrie_4.0.pdf. Zugegriffen am 13.04.2019.
- Gartner. (2019). Umsatz mit Cloud Computing weltweit von 2009 bis 2018 und Prognose bis 2022 (in Milliarden US-Dollar). In *Statista – Das Statistik-Portal*. <https://de.statista.com/statistik/daten/studie/195760/umfrage/umsatz-mit-cloud-computing-weltweit/>. Zugegriffen am 13.05.2019.
- Gluchowski, P. (2016). Business Analytics – Grundlagen, Methoden und Einsatzpotenziale. *HMD Praxis der Wirtschaftsinformatik*, 53(3), 273–286. <https://link.springer.com/content/pdf/10.1365%2Fs40702-015-0206-5.pdf>. Zugegriffen am 06.06.2019.
- Haas, A., & Hofmann, A. (2013). Risiken aus Cloud-Computing-Services: Fragen des Risikomanagements und Aspekte der Versicherbarkeit. No. 74-2013. *FZID Discussion Paper*. <https://www.econstor.eu/bitstream/10419/88163/1/772774323.pdf>. Zugegriffen am 09.05.2019.
- Hertel, M. (2015). Risiken der Industrie 4.0—Eine Strukturierung von Bedrohungsszenarien der Smart Factory. *HMD Praxis der Wirtschaftsinformatik*, 52(5), 724–738. <https://link.springer.com/article/10.1365/s40702-015-0161-1>. Zugegriffen am 16.04.2019.
- Hopfener, A., Timm, C., & Toprak, Y. (2018). *Performance Risk Management: Risikomanagement im Zeitalter von Big Data*. https://www.horvath-partners.com/fileadmin/horvath-partners.com/assets/05_Media_Center/PDFs/Studien-PDFs_fuer_MAT-Download/180806_Performance_Risk_Management_Studienergebnisse_g.pdf. Zugegriffen am 12.05.2019.

- Jacob, O. (2008). *ERP value. ERP Value* (S. 1–22). Berlin/Heidelberg: Springer. https://content.schweitzer-online.de/static/catalog_manager/live/media_files/representation/zd_std_orig_zd_schw_orig/017/911/733/9783540744399_content_pdf_1.pdf. Zugegriffen am 06.04.2019.
- Jacobi, C., & Groher, E. (2019). Beschaffung 4.0. In *Logistik im Wandel der Zeit – Von der Produktionssteuerung zu vernetzten Supply Chains* (S. 545–566). Wiesbaden: Springer Gabler. https://link.springer.com/chapter/10.1007/978-3-658-25412-4_6. Zugegriffen am 03.04.2019.
- Kagermann, H., Lukas, W., & Wahlster, W. (2011). Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4. industriellen Revolution. VDI nachrichten 13.1. https://www.dfgi.de/fileadmin/user_upload/DFKI/Medien/News_Media/Presse/Presse-Highlights/vdinach2011a13-ind4.0-Internet-Dinge.pdf. Zugegriffen am 05.05.2019.
- Kieninger, M., Mehanna, W., & Michel, U. (2015). Auswirkungen der Digitalisierung auf die Unternehmenssteuerung. *Controlling im digitalen Zeitalter*, 3–13. [www.horvath-partners.com](https://www.horvath-partners.com/fileadmin/horvath-partners.com/assets/05_Media_Center/PDFs/deutsch/E_Auswirkungen_Digitalisierung_SCF_Mehanna_Kieninger_Michel.pdf). https://www.horvath-partners.com/fileadmin/horvath-partners.com/assets/05_Media_Center/PDFs/deutsch/E_Auswirkungen_Digitalisierung_SCF_Mehanna_Kieninger_Michel.pdf. Zugegriffen am 25.04.2019.
- Klotz, M., & Dorn, D.-W. (2008). IT-Compliance – Begriff, Umfang und relevante Regelwerke. *HMD Praxis der Wirtschaftsinformatik*, 45(5), 5–14. https://idp.springer.com/authorize/casa?redirect_uri=https://link.springer.com/content/pdf/10.1007/BF03341245.pdf&casa_token=G8cO5U7F23cAAAAAA:Al0e1EMYBm89UkpvrnKzYh4OMl0h_TgQ_V7trHroJzKoA-te85O6TygeHd6a1kst2VWb2q1pTFKNk0B4. Zugegriffen am 23.04.2019.
- Krystek, U. (2007). *Frühauflärung im Rahmen des Risikomanagements von Supply Chains. Risikomanagement in Supply Chains: Gefahren abwehren, Chancen nutzen, Erfolg generieren* (S. 355–364). Berlin. https://books.google.de/books?hl=de&lr=&id=kAg4z1muM7gC&oi=fnd&pg=PA355&dq=Fr%C3%BChaufl%C3%A4rung+im+Rahmen+des+Risikomanagements+von+Supply+Chains&ots=t2ZMhAibCS&sig=C4UWYJH6OOUKdw_X539Uzt2Vx3s. Zugegriffen am 05.04.2019.
- Lasi, H., Fettke, P., Kemper, H. G., Feld, T., & Hoffmann, M. (2014). Industry 4.0. *Business & Information Systems Engineering*, 6(4), 239–242. https://www.researchgate.net/profile/Peter_Fettke/publication/271973139_Industrie_40/links/558bf2c408ae40781c1f7bfa/Industrie-40.pdf. Zugegriffen am 06.06.2019.
- Leveling, J., Schier, A., Luciano, F., & Otto, B. (2014). Konzeption eines proaktiven Risikomanagements in Logistiknetzwerken. *Logistics Journal: Proceedings*, 2014(01). http://www.logistics-journal.de/proceedings/2014/4061/leveling_2014wg1.pdf. Zugegriffen am 17.05.2019.
- Luber, S., & Litzel, N. (2017). *Was ist Digitalisierung?* <https://www.bigdata-insider.de/was-ist-digitalisierung-a-626489/>. Zugegriffen am 20.04.2019.
- Markl, V., Krcmar, H., & Hoeren, T. (2013). *Big Data Management. Innovationspotenzialanalyse für die neuen Technologien für das Verwalten und Analysieren von großen Datenmengen*. http://www.dimta.tu-berlin.de/fileadmin/fg131/Publikation/BDM_Studie/bigdatamanagement-short-DE-finalv099.pdf. Zugegriffen am 07.05.2019.
- McAfee, A., Brynjolfsson, E., Davenport, T. H., Patil, D. J., & Barton, D. (2012). Big data: the management revolution. *Harvard Business Review*, 90(10), 60–68. <http://tarjomefa.com/wp-content/uploads/2017/04/6539-English-TarjomeFa-1.pdf>. Zugegriffen am 12.05.2019.
- Möller, K., Federmann, F., & Knezevic, M. (2016). Predictive Analytics zur kurzfristigen Umsatzprognose – Entwicklung eines Prognosemodells auf Basis von Auftrags eingängen bei der Infineon Technologies AG. *Controlling*, 28(8–9), 535–536. <https://elibrary.vahlen.de/10.15358/0935-0381-2016-8-9-509/predictive-analytics-zur-kurzfristigen-umsatzprognose-jahrgang-28-2016-heft-8-9>. Zugegriffen am 30.04.2019.

- Otto, B., & Österle, H. (2016). *Datenqualität – eine Managementaufgabe. Corporate Data Quality* (S. 1–44). Berlin/Heidelberg: Springer Gabler. https://link.springer.com/chapter/10.1007/978-3-662-46806-7_1. Zugegriffen am 16.04.2019.
- Rohlfs, T. (2018). *Risikomanagement im Versicherungsunternehmen: Identifizierung, Bewertung und Steuerung*. Karlsruhe: VVW GmbH. <https://www.vvw.de>.
- Schröder, M., Findeis, K., & Späth, H. (2019). *Neue Anwendungsmöglichkeiten für das Risikomanagement durch den Einsatz von Big Data – Zwei Fallbeispiele. Logistik im Wandel der Zeit – Von der Produktionssteuerung zu vernetzten Supply Chains* (S. 121–136). Wiesbaden: Springer Gabler. https://link.springer.com/chapter/10.1007/978-3-658-25412-4_6. Zugegriffen am 14.04.2019.
- Steiner, H., & Welker, P. (2016). *Wird der Controller zum Data Scientist? Controlling & Management Review Sonderheft 1-2016* (S. 68–73). Wiesbaden: Springer Gabler. <https://link.springer.com/content/pdf/10.1007%2F978-3-658-13444-0.pdf>. Zugegriffen am 12.05.2019.
- Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business Press. http://www.academia.edu/download/43693253/1300172657060910_it_governance_matrix2535p4.pdf. Zugegriffen am 06.05.2019.
- Wrede, D., Freers, T., & Graf von der Schulenburg, J. M. (2018). Herausforderungen und Implikationen für das Cyber-Risikomanagement sowie die Versicherung von Cyberrisiken—Eine empirische Analyse. *Zeitschrift für die gesamte Versicherungswissenschaft*, 107(4), 405–434. https://doi.springer.com/authorize/casa?redirect_uri=https://link.springer.com/article/10.1007/s12297-018-0425-2&casa_token=tSZF8rBAXxgAAAAA:cKfxJOyXI0W9ex-IQey0IDnjc_118tYTvrG17VhpoZ4tDaXpORvKQA6dSXzTEsTt5HsSzYhmpwJ55w. Zugegriffen am 18.05.2019.
- Zhai, S., & Reinhart, G. (2018). Predictive Maintenance als Wegbereiter für die instandhaltungsrechte Produktionssteuerung. *ZWF Zeitschrift für wirtschaftlichen Fabrikbetrieb*, 113(5), 298–301. <https://www.hanser-elibrary.com/doi/pdf/10.3139/104.111912>. Zugegriffen am 19.04.2019.

Markus Vorbringer ist seit 2013 als Senior Risk Specialist im Global Insurance Risk Management bei der SAP SE am Unternehmenssitz Walldorf tätig. Er unterstützt die Entwicklung und Umsetzung der internationalen Risikofinanzierungsstrategie der SAP sowie die Mitigation von Unternehmensrisiken durch den Einsatz globaler Versicherungsprogramme und die Steuerung damit verbundener Prozesse. Markus Vorbringer studierte Betriebswirtschaft an der Dualen Hochschule in Karlsruhe und hat ein Diplom sowie einen Bachelor-Abschluss.

Thorben Schlätzer hat 2018 seinen Bachelor in Versicherungswesen an der Technischen Hochschule mit den Schwerpunkten Risikomanagement, Bilanzierung und Rückversicherung abgeschlossen. Er konnte seitdem durch Zertifizierungen für die Entwicklung künstlicher Intelligenz seine Fähigkeiten in der Softwareentwicklung vorantreiben und in der Folge als Associate Consultant bei der ISS Software GmbH eigene Software implementieren und die Versicherungswirtschaft zu Themen rund um künstliche Intelligenz beraten. Seit November 2019 ist Herr Schlätzer bei einem staatlich geförderten Start-up, das eine eigen entwickelte künstliche Intelligenz einsetzt, um Dokumente besser zu verstehen und Wissen daraus aufzudecken. Hier übernimmt er einen Teil der Softwareentwicklung sowie hauptsächlich das Marketing und den Vertrieb.

Teil IV

Der Industrieversicherungsmarkt



Versicherungsnehmer und Firmenverbundener Vermittler

14

Jörg Maier und Katharina Faßbender

Zusammenfassung

Industrieunternehmen haben aufgrund ihrer (meist internationalen) Geschäftstätigkeit typischerweise große Risiken. Insbesondere das Zusammenwirken verschiedenster Risiken erhöht die Komplexität und erschwert die Risikosituation. Aus diesem Grund müssen sich Industrieunternehmen mit den vorhandenen und potenziellen Risiken auseinandersetzen, um ihre Existenz und ihre Ziele zu schützen. Dazu muss entschieden werden, wie mit den Risiken umgegangen wird. Ein wichtiger Bestandteil ist dabei der Risikotransfer. Eine Möglichkeit des Risikotransfers ist die Nutzung von Versicherungslösungen. Dafür müssen die Industrieunternehmen als Versicherungsnehmer die Risiken am Versicherungsmarkt platzieren. Eine Möglichkeit ist die Nutzung eines Firmenverbundenen Vermittlers, welcher rechtlich und wirtschaftlich an das Industrieunternehmen gebunden ist und sämtliche Aufgaben und Tätigkeiten eines Versicherungsmaklers ausüben kann. Vorteile hierbei sind zum Beispiel die bestmögliche Kenntnis der relevanten Risiken verbunden mit einer klaren und eindeutigen Interessenlage, die Erfüllung der einschlägigen Vorschriften zur Einnahme von Provisionen und die Transparenz der Kostenstruktur. Außerdem regelt der Firmenverbundene Vermittler in der Regel nicht nur den Versicherungseinkauf, sondern gesamthaft das betriebliche Risikomanagement, zumindest der versicherbaren Risiken. Schlussendlich muss der Versicherungsnehmer den geeigneten Versicherungsvermittler unternehmensindividuell anhand der spezifischen Risiken wählen. Es kann sinnvoll sein, einen Firmenverbundenen

J. Maier (✉)

Voith Assekuranz Vermittlung GmbH, Heidenheim, Deutschland

E-Mail: Joerg.Maier_Heidenheim@t-online.de

K. Faßbender

TH Köln, Institut für Versicherungswesen, Köln, Deutschland

E-Mail: katharina-fassbender@t-online.de

Vermittler für das Hauptgeschäft und gegebenenfalls unterstützend einen Spezialmakler für außergewöhnliche Risiken zu beauftragen.

14.1 Einleitung

Das Industriever sicherungsgeschäft ist ein wichtiger Bestandteil des Versicherungsmarktes. Versicherungsunternehmen grenzen diesen Geschäftsteil oftmals unternehmensindividuell ab. Dabei stellen das Besondere an diesem Versicherungsmarkt die Marktteilnehmer dar. Bei den Versicherungsnehmern handelt es sich in der Regel um große Unternehmen, die zum Beispiel in der Industrie, im Handel und in Dienstleistungen tätig sind. Oftmals betreiben diese dabei internationales Geschäft. Diese Unternehmensaktivitäten bringen große Risiken mit sich, die die Wettbewerbsfähigkeit beeinflussen können und sich meist durch ein hohes potenzielles Schadenausmaß auszeichnen (vgl. Wagner 2018b).

Durch verschiedene Faktoren wie die Globalisierung, Digitalisierung, Beschleunigung und Deregulierung kommt es zusätzlich zu einer Verschärfung der vorhandenen Risikosituation (vgl. Romeike et al. 2013, S. 56). Die Risikosituation der Industrieunternehmen (Versicherungsnehmer) ergibt sich aus der Komplexität der verschiedenen Risiken wie zum Beispiel das Absatz-, Rechtsrisiko, IT Infrastruktur und Reputation (vgl. Romeike et al. 2013, S. 64). Diese Risiken können die Existenz der Firmen bedrohen. Aus diesem Grund ist ein betriebliches Risikomanagement zur Steuerung dieser Risiken unabdingbar (vgl. Robold et al. 2018, S. 13).

Im Rahmen des betrieblichen Risikomanagements werden zur Risikobewältigung diese zum Beispiel versichert. Besonders relevante Versicherungssparten sind die Feuer-/Betriebsunterbrechungs-, Haftpflicht- und Transportversicherung sowie Technische Versicherungen und die Extended-Coverage-Versicherung (vgl. Wagner 2018b). Der Schwerpunkt des folgenden Buchkapitels liegt daher in der Betrachtung der Rolle des Versicherungsnehmers im Zusammenhang mit dem betrieblichen Risikomanagement.

Eine Möglichkeit das betriebliche Risikomanagement und insbesondere das Management der Versicherungen zu betreiben, ist die Integration eines Firmenverbundenen Vermittlers. Der Firmenverbundene Vermittler stellt einen wichtigen Bestandteil des Risikomanagements des Industrieunternehmens dar. Er steht als Bindeglied zwischen dem Industriever sicherer und dem Versicherungsnehmer, gehört aber rein rechtlich und wirtschaftlich zu dem Industrieunternehmen. Er regelt den Versicherungseinkauf für sein Industrieunternehmen (vgl. Farny 2011, S. 751).

Der Firmenverbundene Vermittler managet nicht nur die Gestaltung und Abschlüsse der Versicherungen, sondern auch den Umgang mit Risiken wie zum Beispiel Vermeidung und Verminderung solcher und stellt damit einen wichtigen Faktor für das Risikomanagement des Unternehmens dar (vgl. Berkenkopf 2005). In dem folgenden Beitrag wird daher die Aufgabe und Rolle des Firmenverbundenen Vermittlers in Bezug auf das betriebliche Risikomanagement des Industrieunternehmens herausgestellt. Bei der Einbindung eines

Firmenverbundenen Vermittlers können verschiedene Vorteile erzielt werden, auf die im Folgenden ebenfalls eingegangen wird.

14.2 Versicherungsnehmer im Industrieversicherungsmarkt

14.2.1 Definition des Begriffes „Industrieversicherungsmarkt“

Bei dem Industrieversicherungsmarkt handelt es sich um einen Teil des Versicherungsmarktes. Da die Marktteilnehmer aus der Industrie stammen, sind die Versicherungslösungen und Deckungskonzepte insbesondere auf die Bedürfnisse der Versicherungsnehmer (die Industrieunternehmen) bzw. auf die abzusichernden Industrierisiken abgestimmt (vgl. Mikosch 2005, S. 18 f. und S. 30). Wesentliche Marktteilnehmer sind dabei neben den Versicherungsnehmern, die Industrieversicherer sowie die Versicherungsvermittler (vgl. Robold et al. 2018, S. 14).

Bei dem Versicherungsnehmer bzw. dem Nachfrager handelt es sich um das zu versichernde Großunternehmen aus den Bereichen Industrie, Handel und Dienstleistungen. Aufgrund der speziellen Risikoprofile dieser Firmen, sind die betrieblichen, versicherbaren Risiken im Industrieversicherungsmarkt insbesondere in den Versicherungssparten der Feuer-/Betriebsunterbrechungs-, Haftpflicht- und Transportversicherung, der Technischen Versicherung und der Extended-Coverage-Versicherung angesiedelt. Gleichzeitig ist zu beachten, dass es sich meist um die Versicherung von Großrisiken handelt. Das bedeutet, die Risiken haben zwar eine geringe Eintrittswahrscheinlichkeit, aber dafür ein hohes Schadenausmaß, wenn der Schaden eintritt. Auf die Analyse, Begleitung, Absicherung und Schadenbearbeitung dieser Art von Risiken sind die Industrieversicherer spezialisiert, die als potenzielle Risikoträger auf dem Industrieversicherungsmarkt tätig sind (vgl. Wagner 2018b).

Der Versicherungsvermittler hat dabei die Aufgabe den Versicherungsnehmer zu beraten und ihm eine passende Versicherungslösung bei einem entsprechenden Versicherer anzubieten. Dieser kann jedoch sowohl auf der Nachfrager- als auch auf der Anbieterseite angesiedelt sein, je nachdem welche Interessen er vertritt. Hier gibt es verschiedene Möglichkeiten: Es kann sich zum Beispiel um einen Versicherungsagenten handeln, der wirtschaftlich abhängig vom Versicherer ist. Ein Versicherungsmakler ist dagegen Interessenvertreter des Versicherungsnehmers, also des Industrieunternehmens. Der Firmenverbundene Vermittler stellt eine Besonderheit des Industrieversicherungsmarktes dar, da er rechtlich und wirtschaftlich abhängig von dem Industrieunternehmen ist (vgl. Mikosch 2005, S. 30 ff.).

14.2.2 Versicherungsnehmer

Der Versicherungsnehmer bildet neben dem Versicherungsunternehmen die zweite Vertragspartei in einem Versicherungsvertrag. Es handelt sich dabei um den Nachfrager bzw.

den Käufer von Versicherungsschutz. Dabei kann der Versicherungsnehmer eine natürliche oder juristische Person sein (vgl. Wagner 2018d). Dies bedeutet auch Unternehmen können Versicherungsnehmer sein.

Der Versicherungsnehmer verpflichtet sich durch den Versicherungsvertrag eine Prämie zu zahlen und erhält dafür den Versicherungsschutz für seine Risiken. Das heißt im Schaden- bzw. Leistungsfall wird ihm eine vereinbarte Leistung ausgezahlt (§ 1 VVG). Der Versicherungsnehmer bringt demnach die Risiken in den Versicherungsmarkt ein.

Daneben bestehen für den Versicherungsnehmer gesetzliche und vertragliche Obliegenheiten, die dieser erfüllen muss und weitere vereinbarte Vertragsrechte, die ihm gewährt werden (vgl. Wagner 2018d). Eine vertragliche Obliegenheit in der Sachversicherung kann zum Beispiel die Beachtung von Sicherheitsvorschriften sein, was auch zu einer Vermeidung bzw. Verminderung eines möglichen Schadens beitragen soll (vgl. Wagner 2018c).

Im Industriever sicherungsmarkt unterscheiden die Versicherer in der Regel zwischen folgenden Kundensegmenten: Gewerbe-, Industrie- und Konzernkunden. Dabei gibt es unterschiedliche Abstufungen. Üblicherweise werden diese Abstufungen anhand des Jahresumsatzes des Kunden festgestellt. Hierbei sollte jedoch beachtet werden, dass die Kundensegmente und Abstufungen anhand des Jahresumsatzes je nach betroffenem Industriever sicherer variieren können. Die Einteilung ist also individuell abhängig von dem jeweiligen Risikoträger. Die nachfolgend genannten Grenzen sind daher als ein Beispiel anzusehen. Als Gewerbekunden gelten Firmen mit einem Umsatz zwischen einer Million Euro und fünf Millionen Euro. Dagegen weisen Industrikunden einen Jahresumsatz auf, welcher höher ist. Hier liegt der Umsatz bei bis zu zwischen 300 Millionen Euro und 500 Millionen Euro. Auch kann die Grenze bei bis hin zu einer Milliarde Euro Jahresumsatz liegen. Konzernkunden weisen Jahresumsätze auf, die über die genannten Grenzen hinausgehen. An diesen Abstufungen orientiert sich die Betreuung durch die Versicherer. Dies gilt sowohl für den Vertrieb als auch für die angebotenen Versicherungsprodukte und Deckungskonzepte sowie auch für das kundenbezogene Risikomanagement und die Gestaltung der Rückversicherung.

Typischerweise erhalten Gewerbekunden Standardprodukte, die bis auf wenige spezifische Angaben und Klauseln nicht veränderbar sind. Policien für Industrikunden berücksichtigen das individuelle Risikoprofil des Versicherungsnehmers stärker, enthalten zusätzliche Deckungserweiterungen und höhere Deckungssummen oder Versicherungssummen. Deckungskonzepte für das Segment der Konzernkunden sind maßgeschneiderte Versicherungslösungen hinsichtlich Deckungsumfang, Deckungs- und Versicherungssummen sowie bezüglich der Risikobewertung vor Angebotslegung und der Risikobegleitung während des Bestehens der Kundenbeziehung. Da Konzernkunden international tätig sind bzw. Niederlassungen oder Tochterfirmen im Ausland haben, sind die Versicherer gefordert, mittels ihres Netzwerks an eigenen ausländischen Tochterunternehmen/Niederlassungen oder lokalen Partnerversicherern internationale Versicherungslösungen mit Lokalpolicien anzubieten und einzurichten. Dies wird je nach Ausrichtung der jeweiligen Firmengruppe teilweise auch schon für Kunden im Industriesegment notwendig.

14.3 Versicherungsnehmer im betrieblichen Risikomanagement

14.3.1 Umgang mit Risiken

Durch die operativen Tätigkeiten und den Geschäftsstrategien, die die Industrieunternehmen sowohl im Inland als auch im Ausland tätigen, entstehen Risiken (vgl. Robold et al. 2018, S. 13).

Hinzu kommt, dass es sich in diesem Fall um komplexe *Risiken* handelt, die zum Beispiel Absatz, Recht, IT-Infrastruktur und Reputation betreffen (vgl. Romeike et al. 2013, S. 64). In Abb. 14.1 sind mögliche Risiken für Industrieunternehmen aufgeführt, die in ihrem Zusammenspiel eine hohe Komplexität aufweisen.

Aufgrund der Risikosituation muss sich das Industrieunternehmen klar darüber werden, wie es mit seinen Risiken umgeht. Diese Risiken können die Ziele des Industrieunternehmens bedrohen. Es konzentriert sich dabei unter anderem auf folgende Motive: Gewinnmaximierung betreiben, Arbeitsplätze erhalten, die Unternehmung langfristig betreiben und unter Umständen auch ausbauen. Daher muss es die Arbeitsleistung, Betriebsgebäude, Betriebsinhalte, Fixkosten und die Fortführung des Geschäftsbetriebes nach einem (Versicherungs-)Schaden absichern. Aus diesen verschiedenen Faktoren entsteht der Kundenbedarf des Industrieunternehmens nach Sicherheit. Diesen Wunsch nach Sicherheit sollte ein betriebliches Risikomanagement bieten und soweit möglich und

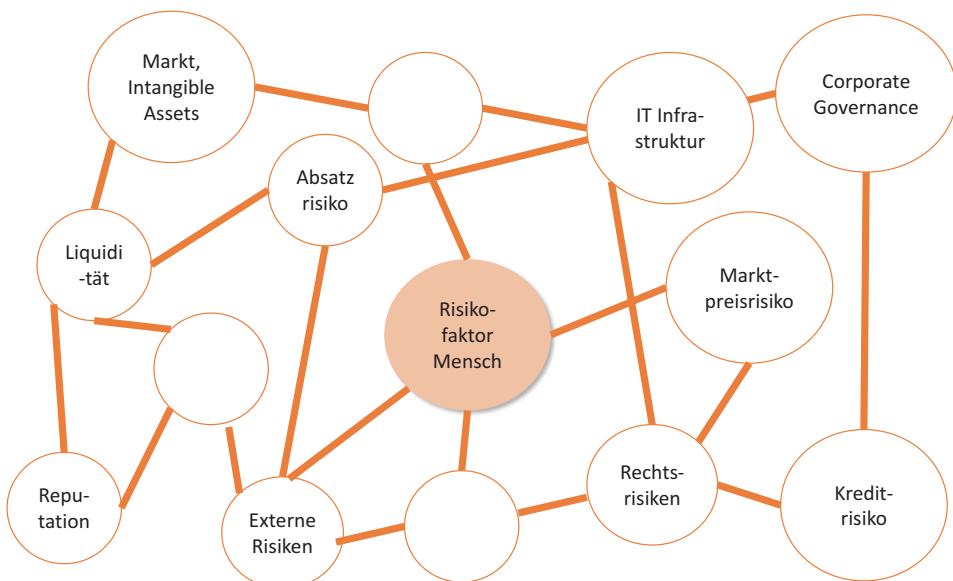


Abb. 14.1 Komplexität von Risiken bei Industrie und Handel. (Quelle: eigene Darstellung in Anlehnung an Romeike et al. 2013, S. 64)

wirtschaftlich sinnvoll über geeignete Versicherungskonzepte verfügen (vgl. Robold et al. 2018, S. 13).

Darüber hinaus besteht auch basierend auf dem KonTraG für alle größeren Unternehmen eine gesetzliche Mindestanforderung an das Risikomanagement, sodass ein Überwachungssystem implementiert werden muss. Dieses soll bestandsgefährdende Entwicklungen frühzeitig erkennen (vgl. § 91 Abs. 2 AktG), Transparenz schaffen und Risikobewältigungsmaßnahmen wie zum Beispiel Versicherungen einrichten.

Um den Kundenbedarf nach Sicherheit zu gewährleisten und die gesetzlichen Regelungen zu erfüllen, implementiert das Industrieunternehmen ein betriebliches Risikomanagement mit unter anderem einer systematischen und laufenden Risikoanalyse der Geschäftsabläufe und einem Risikomanagementprozess im Unternehmen (vgl. Romeike et al. 2008, S. 74).

In diesem Zusammenhang wird sich das Unternehmen darüber klar, welche Risiken sich in den operativen Tätigkeiten und in dem Geschäftsmodell befinden, wie diese in ihrer Schwere zu bewerten sind und wie sich diese gemeinsam als Risikokapital auswirken und somit die Risikotragfähigkeit des Unternehmens belasten (vgl. Rohlf 2018, S. 75 f.).

Anschließend muss sich das Unternehmen überlegen, wie es mit den Risiken umgehen will. Hier bestehen mehrere Möglichkeiten. Einzelne Risiken können vermieden werden, indem zum Beispiel Betriebsabläufe verändert oder ersetzt werden. Auch können Risiken vermindert werden, sodass sie für das Unternehmen tragfähig werden (vgl. Rohlf 2018, S. 258 und 262). Ein Beispiel hierfür wäre die Installation einer Sprinkleranlage, um einen Brand und den daraus resultierenden Feuerschaden zu begrenzen.

Ein wesentlicher Bestandteil des Risikomanagements ist der Transfer von Risiken. Dabei werden Risiken auf Dritte übertragen. Dazu gehört auch der Risikotransfer durch Versicherungen (vgl. Romeike et al. 2013, S. 143). Dies ist oftmals der wirtschaftlich sinnvollste Weg der Absicherung von Risiken (vgl. Mertens 2019). Hierfür muss das Unternehmen das Risiko am Versicherungsmarkt platzieren. Dann wird ein Versicherungsvertrag abgeschlossen, sodass das Industrieunternehmen in die Position des Versicherungsnehmers tritt. Da sich das Versicherungsmanagement an der Unternehmensstrategie orientiert, ist es unternehmensindividuell zu gestalten (vgl. Mertens 2019).

Versicherungslösungen müssen nicht alleinstehend genutzt werden. Es gibt die Möglichkeit innerhalb des Versicherungsmanagements andere Maßnahmen der Risikobewältigung zu kombinieren, zum Beispiel die Optimierung von Verträgen mit Lieferanten und Kunden (vgl. Romeike et al. 2013, S. 144).

Daneben gibt es auch die Möglichkeit Versicherungsprogramme zu nutzen, um große oder multinationale Risiken abzudecken. Dazu werden mehrere Versicherungsverträge kombiniert. Dies wird häufig im Zusammenhang mit internationalen Risiken und in den Sparten der Transport-, Sach-, Haftpflicht- und Technischen Versicherung genutzt. Hierbei gibt es einen Hauptvertrag, der für alle Länder einheitliche Versicherungsbedingungen formuliert und in dem Land des Hauptsitzes belegen ist. Darauf aufbauend werden für die einzelnen Länder lokale Grundpolices angefertigt, die den spezifischen Anforderungen des jeweiligen Landes hinsichtlich Risikoanalyse vor Ort, Vertragsbearbeitung,

Schadenregulierung usw. genügen. In einem Schadensfall werden dann die lokalen Deckungssummen und -inhalte zur Verfügung gestellt. Falls diese nicht greifen, kommt die Hauptpolice zum Einsatz (vgl. Mikosch 2005, S. 218).

Das Unternehmen muss sich also nach der Risikoidentifizierung die Frage stellen, wie es mit den vorhandenen und zukünftigen Risiken umgeht. Sowohl eigene Maßnahmen und Selbsttragung der Risiken bis hin zu einem Risikotransfer sind denkbare Möglichkeiten.

14.3.2 Versicherungseinkauf als organisatorische Fragestellung

Entscheidet sich das Unternehmen zu der Versicherungslösung als Risikotransfer, muss es seine Risiken am Versicherungsmarkt platzieren. Hierbei gibt es unterschiedliche Möglichkeiten, wie es den Versicherungseinkauf im eigenen Unternehmen organisieren kann.

Im Rahmen von Corporate Governance, also dem rechtlichen und faktischen Ordnungsrahmen eines Unternehmens für eine verantwortungsvolle Unternehmensführung und -überwachung, wird auch das Risikomanagement betrachtet (vgl. Rohlfs 2018, S. 34 und 49). Hierbei geht es unter anderem darum, wie das Risikomanagement in die Unternehmensabläufe integriert wird. Im Rahmen von Corporate Governance muss in der Aufbauorganisation eine Funktionstrennung von bestimmten Schlüsselfunktionen erfolgen. Dazu gehört auch das Risikomanagement. Das bedeutet, dass Personen, die die Risiken eingehen, nicht das weitere Risikomanagement betreiben dürfen (vgl. Rohlfs 2018, S. 68 f.). Darüber hinaus wird deutlich, dass das Risikomanagement einschließlich des Versicherungsmanagements eine „originäre Leitungspflicht des Vorstands“ darstellt (vgl. Romeike et al. 2013, S. 148).

Konkret bedeutet dies für das Industrieunternehmen als Versicherungsnehmer, dass die Geschäftsleitung die Geschäfts- und Risikostrategie, Leitlinien für das Risikomanagement und weitere Elemente wie zum Beispiel Risikotoleranz und -früherkennung festlegt. Davor getrennt erfolgt die Umsetzung dessen zum Beispiel die Identifizierung, Analyse und Steuerung von Risiken (vgl. Rohlfs 2018, S. 69).

Im Rahmen des Versicherungseinkaufs wird nicht nur der tatsächliche Einkauf operativ durchgeführt, sondern es wird auch herausgearbeitet, was gekauft wird. Konkret bedeutet dies Folgendes: Das jeweils benötigte Versicherungsprodukt wird hinsichtlich der sich aus der vorausgegangen Risikoanalyse und -bewertung ergebenden Absicherungsbedürfnisse des Unternehmens gestaltet. Die Versicherungsbedingungen bzw. die Rahmenbedingungen des Vertrages werden zum Beispiel in den Punkten Prämienzahlung, Leistungserbringung, vorvertragliche Pflichten, Ausschlüsse, Deckungserweiterungen, vertragliche Obliegenheiten und weiteren Hauptleistungen des Produktes ausgestaltet (vgl. Wagner 2018a).

Der Versicherungsnehmer hat verschiedene Optionen das Versicherungsmanagement und speziell den Versicherungseinkauf in seiner Organisation zu integrieren. Eine erste Möglichkeit ist die, dass eine unternehmensinterne Abteilung damit betraut wird. Das bedeutet, dass das Unternehmen eine Abteilung im Unternehmen schafft, die sich

ausschließlich mit dem Versicherungseinkauf und dem weiteren Versicherungsmanagement beschäftigt. Ein Vorteil dieser Organisation ist es, dass der Versicherungseinkauf damit rechtlich und wirtschaftlich abhängig ist und eine enge Verbindung zum Unternehmen aufweist. So ist die Weisungsgebung entsprechend direkt möglich. Je nachdem kann es als Schlüsselfunktion auch direkt unter dem Vorstand angesiedelt werden, sodass dieser Effekt verstärkt wird. Ein weiterer Vorteil einer unternehmensinterne Abteilung ist, dass internes Know-how aufgebaut wird und sich die eigenen Mitarbeiter exklusiv auf das Unternehmen konzentrieren. Der Nachteil der Organisation des Versicherungseinkaufs über eine unternehmensinterne Abteilung kann sein, dass es zu einer sogenannten Betriebsblindheit bei den Mitarbeitern kommt. Außerdem besteht die Gefahr, dass den Mitarbeitern gewisse Spezialkenntnisse fehlen, die intern auch nicht ohne weiteres erworben werden können (vgl. Mikosch 2005, S. 31).

Daneben kann das Unternehmen den Versicherungseinkauf in Form einer eigenständigen Gesellschaft zum Beispiel einer GmbH organisieren. Hierbei handelt es sich um einen Firmenverbundenen Vermittler, der rechtlich und wirtschaftlich von dem Unternehmen abhängig ist. Die Rolle und Aufgaben sowie Vorteile der Organisation über einen Firmenverbundenen Vermittler werden später näher erläutert.

Neben den zwei genannten Optionen kann das Industrieunternehmen den Versicherungseinkauf auch über einen externen Versicherungsvermittler bzw. Versicherungsmakler steuern. Dieser ist dann unabhängig von dem Unternehmen, nur bedingt weisungsgebunden und steht daher aber auch nicht unmittelbar in der Interessensphäre des Unternehmens. Dieser erledigt das Versicherungsmanagement als Dienstleistung für das Unternehmen. Typischerweise weist der Versicherungsmakler externes und fachspezifisches Know-how sowie entsprechende personelle Kapazitäten auf.

14.3.3 Platzierung von Risiken am Versicherungsmarkt

Bei der Platzierung der Risiken am Versicherungsmarkt muss der geeignete Industriever sicherer ausgewählt werden. Hierbei ist eine Reihe von Kriterien zu beachten.

Bei der Auswahl des Industriaversicherers ist die generelle Risikotragfähigkeit zu berücksichtigen. Hierzu sind zum Beispiel Informationen des Versicherungsunternehmens wie der Geschäftsbericht, die generelle und spezifische Zeichnungspolitik von Risiken und Industriezweigen sowie das Rating zur Beurteilung hinzuzuziehen.

Es ist zu beachten, dass das im Versicherungseinkauf gestaltete Produkt inklusive der Vertragsbedingungen zu den angebotenen Versicherungsbedingungen des Industriaversicherers passend sein muss. Außerdem muss die angebotene Kapazität der Deckungssummen und der weiteren Limite, den Ausmaßen des Risikos genügen und dieses adäquat absichern können. Auch muss der Versicherungsnehmer erstens bereit sein, den geforderten Preis bzw. die zu entrichtende Prämie zu bezahlen und zweitens muss diese in einem angemessenen Verhältnis zur gebotenen Absicherung stehen.

Zu Versicherungsleistungen gehören nicht nur die Entschädigungen im Schadensfall, sondern auch weitere Serviceleistungen, die für einen Kauf ausschlaggebend sein können. Der Versicherungsnehmer sollte also auch das Angebot des Versicherers hinsichtlich der gebotenen Serviceleistungen prüfen. Dazu gehören die Möglichkeiten des Industriever sicherers, eine Unterstützung für das betriebliche Risikomanagement anzubieten. Auch eine Beratung bei anfallenden fachlichen Fragestellungen kann relevant sein. Ein weiterer wichtiger Punkt gerade im heutigen Zeitalter ist der Service zum Thema Digitalisierung und den damit verbundenen Risikoänderungen. Auch das generelle Verhalten des Versicherers im Schadenfall und seine Kompetenz im Management und der Regulierung des Schadens sind nicht zu vernachlässigen.

Diese Kriterien und unternehmensspezifischen Anforderungen müssen bei der Auswahl des Versicherers gegeneinander abgewogen werden. Alle Wunschkriterien zu erfüllen, wird eine Schwierigkeit darstellen. Das Unternehmen sollte hinsichtlich seiner Präferenzen die beste Möglichkeit wählen.

Je nachdem wie der Versicherungseinkauf organisiert ist, kann das Unternehmen die Kriterien über eine unternehmensinterne Abteilung unter den oben genannten Vor- und Nachteilen prüfen lassen. Eine andere Möglichkeit ist es einen Versicherungsvermittler mit dieser Aufgabe zu trauen. Bei der Auswahl des Versicherungsvermittlers sind ebenfalls Anforderungen zu stellen. So sind unter anderem eine gewisse wirtschaftliche Unabhängigkeit, Professionalität, Objektivität, ein vorhandenes Netzwerk, Seriosität, Kompetenz und Internationalität wichtige Faktoren, um einen geeigneten Versicherungsvermittler für die eigenen Bedürfnisse auszuwählen.

Hierbei gibt es verschiedene Möglichkeiten: Bspw. kann ein Versicherungsvertreter, auch Versicherungsagent, beauftragt werden. Der Versicherungsvertreter ist von dem Versicherungsunternehmen betraut, Versicherungsverträge zu schließen und zu vermitteln (§ 59 Abs. 2 VVG). Er kann auch von mehreren Versicherungsunternehmen betraut sein und wird dann Mehrfachagent genannt. Dieser ist durch seine Beauftragung durch den Versicherer auch in der Interessensphäre dessen angesiedelt. Dies wäre ein Kritikpunkt gegen die Beauftragung eines Versicherungsagenten. Dadurch, dass ein Einfirmenvertreter auch nur die Produkte dieses Versicherungsunternehmens vermittelt, hat er gerade im Falle von nicht standardisierten Industrierisiken möglicherweise ein begrenztes Angebot. Darüber hinaus fehlt unter Umständen auch das fachliche Know-how insbesondere im Fall von Spezialrisiken (vgl. Mikosch 2005, S. 30 f.).

Eine weitere Möglichkeit für die Platzierung von Risiken kann die Beauftragung eines Versicherungsmaklers sein. Die Vorteile hierbei sind, dass der Versicherungsmakler Interessensvertreter des Kunden ist. Meistens bieten diese auch weitere Dienstleistungen mit Spezialwissen an. So ist ein Fullservice für das betriebliche Risikomanagement nicht unüblich. Auch haben Versicherungsmakler meist internationale Netzwerke, die sie nutzen können (vgl. Mikosch 2005, S. 34). Hierzu müsste der Versicherungsmakler jedoch nach unternehmensindividuellen Kriterien näher beurteilt werden. Auch gibt es sogenannte Spezialmakler, die in den unterschiedlichen Sparten oder Fachbereichen tiefe

Spezialkenntnisse aufgebaut haben und somit zu den jeweiligen Themen noch zielgerichteter beraten können.

Der Firmenverbundene Vermittler ist auch ein Versicherungsvermittler, über den der Versicherungseinkauf bzw. das Versicherungsmanagement gesteuert werden kann. Der Firmenverbundene Vermittler wird samt seinen Aufgaben und Rollen im nächsten Abschnitt näher beleuchtet.

Das Unternehmen muss sich am Schluss darüber im Klaren sein, nach welchen der oben genannten Kriterien es den Versicherer und einen möglichen Versicherungsvermittler auswählt. Auch können für verschiedene Risiken verschiedene Möglichkeiten gewählt werden. Beispielsweise kann ein Firmenverbundener Vermittler beschäftigt werden, der das Hauptgeschäft des Versicherungsmanagements übernimmt und für speziellere Risiken wird dann ein (Spezial-)Makler ausgewählt oder unterstützend hinzugezogen.

14.4 Firmenverbundene Vermittler im Industrieversicherungsmarkt

14.4.1 Definition des Begriffes „Firmenverbundener Vermittler“

Grundsätzlich ist ein Versicherungsvermittler eine natürliche oder juristische Person, die Versicherungen zwischen dem Versicherungsunternehmen und dem Kunden bzw. Versicherungsnehmer vermittelt. Aufgaben des Versicherungsvermittlers sind nicht nur die Erstberatung und der Verkauf der Versicherungen, sondern auch die weitere Betreuung und Beratung zum Beispiel hinsichtlich Vertragsänderungen oder Schadensfällen. Der Versicherungsvermittler erhält für seine Tätigkeit in der Regel eine Provision von dem Versicherungsunternehmen. Ein Versicherungsvermittler benötigt zur Ausübung seiner Tätigkeit eine Erlaubnis durch die jeweils zuständige Industrie- und Handelskammer und es ist eine Eintragung in das Vermittlerregister des Deutschen Industrie- und Handelskammertag e. V. notwendig (vgl. Wagner 2018e).

Oftmals erfolgt der Versicherungseinkauf im gewerblichen Bereich also zum Beispiel bei Industrieunternehmen über eigens beauftragte Beschaffungsorgane wie den Firmenverbundenen Vermittler (vgl. Farny 2011, S. 745 f.). Der Firmenverbundene Vermittler ist ein Versicherungsvermittler, der jedoch rechtlich und wirtschaftlich von dem Versicherungsnehmer abhängig ist (vgl. Mikosch 2005, S. 32 f.). Die rechtliche Abhängigkeit entsteht dadurch, dass das Industrieunternehmen Eigentumsrechtsverhältnisse an dem Vermittlerunternehmen hält. Eine zusätzliche wirtschaftliche Abhängigkeit kann durch die Zahlung des Versicherungsnehmers in Form eines Honorars für die Tätigkeit des Firmenverbundenen Vermittlers entstehen (vgl. Beenken 2017, S. 33).

Häufig kommt dies bei Industrieunternehmen vor, die so ihre früher rechtlich unabhängige Versicherungsabteilung auslagern. Vertragsrechtlich sind sie als Makler oder (Mehrfach-)Vertreter, jedoch wirtschaftlich als Beschaffungsorgan des Industrieunternehmens tätig (vgl. Farny 2011, S. 751). Da der Firmenverbundene Vermittler zu dem Industrieun-

ternehmen gehört bzw. abhängig von diesem ist, erhält das Unternehmen als Versicherungsnehmer indirekt die Provisionen. Daher gelten hier bzgl. des Provisionsabgabeverbots besondere Bestimmungen.

Der Firmenverbundene Vermittler übernimmt neben seiner Tätigkeit der Beschaffung von Versicherungsschutz auch Aufgaben des Risikomanagements wie zum Beispiel die Risikoermittlung, die Absicherung und die Abwicklung von Schaden- und Leistungsfällen für das Industrieunternehmen (vgl. Farny 2011, S. 751).

Neben der Versicherungsvermittlung und dem betrieblichen Risikomanagement für das Industrieunternehmen betreiben die Firmenverbundenen Vermittler unter Umständen auch das Belegschaftsgeschäft. Das bedeutet, dass sie den privaten Versicherungsschutz der Angestellten des Unternehmens vermitteln und verwalten. Dadurch können zum Beispiel günstigere Konditionen erzielt werden, da Gruppentarife abgeschlossen werden können. Dies ist zum Beispiel in der Unfall-, Berufsunfähigkeits- oder Kraftfahrzeugversicherung der Fall. Der Firmenverbundene Vermittler erhält dafür Provisionen und das Industrieunternehmen steigt in seiner Attraktivität als Arbeitgeber (vgl. Berkenkopf 2005).

Betreiben die Firmenverbundenen Vermittler neben dem Geschäft für ihr eigenes Unternehmen auch zum Beispiel noch Vermittlertätigkeiten für andere Unternehmen, dann kann von echter Vermittlungstätigkeit gesprochen werden (vgl. Farny 2011, S. 751).

14.4.2 Abgrenzung Cost Center und Profit Center

Cost Center und Profit Center sind die Bezeichnung für organisatorische Einheiten im Unternehmen und dienen zur internen Steuerung. Die Einteilung gemäß Cost und Profit Center hat den Vorteil der gezielteren Steuerung der Unternehmenseinheiten und der Förderung des unternehmerischen Denkens und Handels in diesen Einheiten (vgl. Schawel et al. 2012, S. 210).

In Abb. 14.2 sind die wichtigsten Merkmale von Cost und Profit Center aufgelistet.

Der Firmenverbundene Vermittler muss nicht nur ausschließlich für das zugehörige Unternehmen arbeiten, sondern kann auch externe Kunden beraten. Dazu zählen sowohl Privatkunden als auch andere Unternehmern Kunden (vgl. Berkenkopf 2005). Ein Firmenverbundener Vermittler kann also als Cost oder als Profit Center angesehen werden je nachdem, ob dieser ausschließlich für das eigene Unternehmen tätig ist oder auch für externe Kunden.

Zählt ein Firmenverbundener Vermittler als Cost Center, erwirtschaftet er lediglich Umsätze durch die Honorarzahlung des Industrieunternehmens und die Provisionen des Versicherungsunternehmens. Anhand der Kriterien kann daher davon ausgegangen werden, dass dieser zwar eine Marktnähe aufweist, aber durch seine hauptsächliche Tätigkeit für das Industrieunternehmen eine geringere (geschäftliche) Interaktion mit anderen Marktakteuren hat.

Im Falle des Firmenverbundenen Vermittlers als Cost Center legt das Unternehmen den Fokus auf die Kosteneinhaltung je Geschäftsperiode. Es ist davon auszugehen, dass der

Cost Center	Profit Center
<ul style="list-style-type: none"> • Ausschließlich unternehmensinterne Umsätze • Marktnähe, aber geringere geschäftl. Interaktion mit anderen Marktakteuren • Fokus: Kosteneinhaltung des verfügbaren Budgets in einer Periode • Stark in betriebliche Abläufe eingebunden • Einsatzgrund: Leistungen, die nicht am externen Markt angeboten werden 	<ul style="list-style-type: none"> • Unternehmensinterne und unternehmensexterne Umsätze • Marktnähe, aber höhere geschäftl. Interaktion mit anderen Marktakteuren • Fokus: Maximierung des Gewinns bzw. Deckungsbeitrages einer Periode • Arbeitsweise selbständig und eigenverantwortlich • Einsatzgrund: Leistungen, die auch am externen Markt angeboten werden (wettbewerbsfähige Kompetenz)

Abb. 14.2 Abgrenzung Cost und Profit Center. (Quelle: eigene Darstellung in Anlehnung an Schawel et al. 2012, S. 211 f.)

Firmenverbundene Vermittler in diesem Fall vorrangig stark in die betrieblichen Abläufe eingebunden ist. Grund für die Regelung des Firmenverbundenen Vermittlers als Cost Center könnte sein, dass das Industrieunternehmen durch dessen Einrichtung die Kosten durch zum Beispiel externe Versicherungsvermittler wie Versicherungsmakler vermeiden will.

Wird der Firmenverbundene Vermittler dagegen als Profit Center gewertet, erwirtschaftet er nicht nur Umsätze durch das eigene Unternehmen, sondern auch durch externe Kunden zum Beispiel andere Industrieunternehmen oder auch Privatkunden. In diesem Fall ist eine hohe Nähe zum Industrie- bzw. Versicherungsmarkt durch die geschäftliche Interaktion mit anderen Marktakteuren zu beobachten.

Das Industrieunternehmen legt neben der Kosteneinhaltung auch die Absicht der Gewinnmaximierung zugrunde. Der Grund für die Einrichtung des Firmenverbundenen Vermittlers als Profit Center könnte demnach sein, dass das Industrieunternehmen nicht nur Kosten einsparen möchte, sondern auch Gewinn am Markt durch andere Versicherungsnehmer erzielen möchte.

14.4.3 Provisionsabgabeverbot

Das Provisionsabgabeverbot regelt, dass Versicherungsunternehmen und Versicherungsvermittler sowie deren Angestellte keine Sondervergütungen an die Kunden auszahlen dürfen. Zu den Kunden zählen der Versicherungsnehmer, der Versicherte und auch die

Bezugsberechtigten (§ 48b Abs. 1 VAG). Unter Sondervergütungen versteht der Gesetzgeber unter anderem die Abgabe (von Teilen) der Provision an den Kunden aber auch andere Sach- und Dienstleistungen außerhalb der Versicherungsleistung oder die Rabattierung auf Waren und Dienstleistungen von mehr als 15 Euro pro Versicherungsverhältnis und Kalenderjahr (§ 48b Abs. 2 VAG).

Nach dem Provisionsabgabeverbot ist es zum Beispiel verboten, dass der Versicherungsvermittler auf seine Vergütung verzichtet, damit der Versicherungsnehmer eine Ermäßigung auf die Prämie erhält (vgl. Olbrich 2009, S. 240).

Bei einem Verstoß der Regelung handelt es sich um eine Ordnungswidrigkeit aufgrund derer entsprechende Konsequenzen durch die BaFin drohen (vgl. Olbrich 2009, S. 240). Es können Geldbußen bis zu 100.000 Euro angeordnet werden (§ 144a Abs. 1 Nr. 2 und 3 VAG). Die Strafe trifft dabei jedoch nicht den Versicherungsnehmer, sondern den Versicherungsvermittler (§ 134 BGB). Da der Firmenverbundene Vermittler jedoch dem Versicherungsnehmer zugehörig ist, trifft in diesem Fall die Strafe faktisch auch den Versicherungsnehmer.

Das Provisionsabgabeverbot wurde eingeführt, um zu verhindern, dass einzelne Versicherungsnehmer bevorzugt werden und somit eine Gleichbehandlung nicht gegeben wäre. Außerdem verfolgt der Gesetzgeber das Ziel, dass Prämien nicht durch höhere Provisionszahlungen steigen. Versicherungsvermittler sollen Teile ihres Einkommens nicht abgeben. Vielmehr aber ist das Motiv des Gesetzgebers, Markttransparenz und Qualität der Beratung des Versicherungsvermittlers durch das Zahlen einer entsprechenden Vergütung (die Provision) sicherzustellen (vgl. Winter 2007, S. 666).

Die Kritik an dem Verbot lautet, dass es sich hierbei um eine Wettbewerbseinschränkung handelt. Der Versicherungsvermittler hat dadurch weniger Möglichkeiten, den Preis flexibel zu gestalten und zum Beispiel Rabatte zu vergeben. Eine Preisfindung durch ein Übereinkommen von Angebot und Nachfrage ist somit nur noch eingeschränkt möglich. Darüber hinaus ist die ökonomische Wirkung des Provisionsabgabeverbots bei den Kritikern umstritten (vgl. Olbrich 2009, S. 240).

Eine Ausnahme in dem Provisionsabgabeverbot besteht darin, wenn Versicherungsvermittler die Provision mit einem anderen Vermittler teilen, der mit in das Geschäft eingebunden ist. Daher können Industrieunternehmen Firmenverbundene Vermittler einstellen und verstößen auf diese Weise nicht gegen das Provisionsabgabeverbot (vgl. Berkenkopf 2005). indirekt erhält der Versicherungsnehmer, also das Industrieunternehmen, aufgrund der rechtlichen Abhängigkeit des Firmenverbundenen Vermittlers Teile der Provisionszahlungen des Versicherungsunternehmens.

Im Zusammenhang mit der Einrichtung eines Firmenverbundenen Vermittlers sind daher besondere Regelungen zu beachten, um nicht dem Verstoß gegen das Provisionsabgabeverbot ausgesetzt zu werden. Aktuell prüft die Einhaltung der relevanten Vorschriften noch die Wiesbadener Vereinigung (vgl. Olbrich 2009, S. 240).

Die Wiesbadener Vereinigung ist ein durch die deutsche Versicherungswirtschaft gegründetes Abkommen, welches Tätigkeitsmerkmale des firmenverbundenen Vermittlers



Abb. 14.3 Tätigkeitsmerkmale des Firmenverbundenen Vermittlers nach der Wiesbadener Vereinigung. (Quelle: eigene Darstellung in Anlehnung an Olbrich 2009)

festlegt. Werden diese erfüllt, dürfen Firmenverbundene Vermittler eine Provision auch für das firmeneigene Versicherungsgeschäft erhalten (vgl. Olbrich 2009, S. 241). In Abb. 14.3 sind diese Tätigkeitsmerkmale aufgelistet.

Sind die in der Abbildung aufgeführten Voraussetzungen nicht gesamthaft erfüllt, kommt es zu einem Verstoß gegen das Provisionsabgabeverbot.

Es gibt darüber hinaus zwei weitere Möglichkeiten, nicht gegen das Provisionsabgabeverbot zu verstößen: Die Vereinbarung eines Beratungsvertrags oder eines Tippsgebervertrags. Das Versicherungsunternehmen kann einen provisionsfreien Nettotarif anbieten. Vermittelt der Firmenverbundene Vermittler dem Unternehmen einen solchen Tarif, dann liegt kein Verstoß des Gesetzes vor, wenn entsprechend eines Beratungsvertrages ein Honorar vereinbart wurde. Dieses Honorar darf nicht an den Versicherungsnehmer zurückgezahlt werden (vgl. Olbrich 2009, S. 241).

Im Falle des Tippsgebervertrages kann die Provision an den Versicherungsnehmer zurückgegeben werden, denn der Versicherungsvermittler darf dem Kontaktvermittler zu einem Interessenten Provision für die Vermittlung des Kunden übermitteln (vgl. Olbrich 2009, S. 241).

Die Wiesbadener Vereinigung, die bisher diese Einhaltung kontrolliert hat, wurde aufgrund der veränderten Rechtslage zum 30. Juni 2019 aufgelöst (vgl. versicherungsjournal.de 2019). Da Versicherungsvermittler nach dem IDD-Umsetzungsgesetz gemäß § 34d Abs. 1 GewO das Provisionsabgabeverbot gemäß § 48b VAG einhalten müssen, ist nun die jeweilige Industrie- und Handelskammer für die Kontrolle der Einhaltung zuständig.

14.4.4 Wesentliche Vorteile des Einsatzes eines Firmenverbundenen Vermittlers

Ein wesentlicher Vorteil eines Firmenverbundenen Vermittlers ist der angesprochene Umgang mit dem Provisionsabgabeverbot. Darüber hinaus ist ein weiterer Vorteil des Einsatzes eines Firmenverbundenen Vermittlers, dass die Kostenstruktur unter Umständen klarer ist als bei externen Versicherungsmaklern. Die Kostenstrukturen können von dem Versicherungsnehmer bei einem Firmenverbundener Vermittler offen eingesehen werden. Das bedeutet, es besteht eine höhere Kostentransparenz im Gegensatz zum Rückgriff auf externe Markakteure, wo Preise zum Beispiel erst ausgehandelt werden müssen und keine Kenntnis über die Provision besteht (vgl. Mertens 2019). Darüber hinaus ist ein Einwirken auf die Kostenstruktur im Falle eines Firmenverbundenen Vermittlers unter Umständen wahrscheinlicher und es kann ein stärkerer Fokus auf die Kosteneinhaltung je Geschäftsperiode gelegt werden.

Ein weiterer Vorteil ist der Aufbau von firmeninternem Know-how (vgl. Mikosch 1991, S. 42). Dadurch sind die Mitarbeiter, die sich mit der wichtigen Funktion des Risikomanagements und der Risikoplatzierung am Versicherungsmarkt beschäftigen, in der Regel eher vor Ort und verfügbar. Darüber hinaus kann auf Experten im eigenen Unternehmen wie zum Beispiel Juristen und Steuerberater zurückgegriffen werden (sofern diese vorhanden sind), ohne dass externes Know-how teuer eingekauft werden muss. Ein weiteres Argument ist die höhere Akzeptanz im eigenen Unternehmen des Firmenverbundenen Vermittlers gegenüber anderen Einheiten, mit denen eine Zusammenarbeit erforderlich ist (vgl. Mertens 2019).

Auch hinsichtlich möglicher Interessenkonflikte ist der Einsatz eines Firmenverbundenen Vermittlers sinnvoll. Da der Firmenverbundene Vermittler zugehörig zu dem Industrieunternehmen ist und somit den Interessenvertreter des Versicherungsnehmers darstellt, wird er bei der Aushandlung des Versicherungsvertrages auch die Interessen seines Kunden vor dem Versicherungsunternehmen stärker als ein externer Versicherungsmakler vertreten (vgl. Mertens 2019). Daher ist die Wahrscheinlichkeit eines passenden und maßgeschneiderten Versicherungsschutzes hoch. Das wird durch die internen Kenntnisse des Firmenverbundenen Vermittlers verstärkt. Dieser kennt die Risiken aus erster Hand und beschäftigt sich auch im Idealfall im Rahmen des betrieblichen Risikomanagements mit dem gesamthaften Risikoumgang. Dadurch hat er einen Rundumblick über das gesamte Risikomanagement und kann auf mögliche Problemstellungen oder veränderte Umweltumstände angemessen und schnell reagieren.

Auch können Aufgaben, bei denen kein Outsourcing möglich ist, von dem Firmenverbundenen Vermittler übernommen werden. Dazu gehören unter anderem folgende Tätigkeiten:

- Ermittlung von Versicherungssummen,
- Prämienallokation an Tochterunternehmen,
- Handling von Selbstversicherungsmodellen,

- Erfassung von Schadeninformationen,
- Schadenprävention und
- internes Risikomanagement (vgl. Mertens 2019).

Ein weiterer Punkt ist, dass Industriever sicherer dem Firmenverbundenen Vermittler eher Sonderbedingungen gewähren, da dieser diese nur für sein eigenes Unternehmen nutzt und nicht wie ein Versicherungsmakler auch für andere Kunden aushandeln möchte. Dies ist vor allem der Fall, wenn der Firmenverbundene Vermittler als Cost Center agiert.

Ein Firmenverbundener Vermittler bringt zwar viele Vorteile mit sich, aber es müssen auch mögliche Gefahren berücksichtigt werden. Sowohl eine Betriebsblindheit und ein Know-how, welches sich ausschließlich auf das entsprechende Unternehmen beschränkt, kann dabei eine Spannung hervorrufen (vgl. Mikosch 1991, S. 42).

14.4.5 Aufgabe und Rolle des Firmenverbundenen Vermittlers im betrieblichen Risikomanagement

Der Firmenverbundene Vermittler kann eine wichtige Rolle im betrieblichen Risikomanagement des Industrieunternehmens übernehmen. In den meisten Fällen übernimmt der Firmenverbundene Vermittler nicht nur die Versicherungsvermittlung bzw. das Versicherungsmanagement für sein Industrieunternehmen, sondern auch alle anderen Aufgaben, die mit dem betrieblichen Risikomanagement zu tun haben. Dazu gehören der komplette Bereich der Risikoermittlung, die Absicherung und auch der Schaden-/Leistungsbereich (vgl. Robold et al. 2018, S. 13).

Mithilfe von Abb. 14.4 wird der Risikomanagementprozess aufgegriffen, um anhand dessen die Aufgabe und Rolle des firmenverbundenen Vermittlers im betrieblichen Risikomanagement zu erläutern.

Implementiert ein Industrieunternehmen einen Firmenverbundenen Vermittler nicht nur zur Platzierung der Risiken am Versicherungsmarkt, sondern auch für die Durchführung des betrieblichen Risikomanagements, können die einzelnen Schritte des Risikomanagements als Aufgabe des Firmenverbundenen Vermittlers angesehen werden. Er durchläuft die oben genannten Phasen des Risikomanagementprozesses und entscheidet somit, wie mit Risiken planmäßig und systematisch umgegangen wird (vgl. Möbius et al. 2013, S. 47).

Dazu gehört auch, dass der Firmenverbundene Vermittler für das Industrieunternehmen eine Gesamtstrategie zur Verbesserung der Risikostruktur, der Integration von Einzelsystemen, der Eingrenzung der wesentlichen Risiken, der Früherkennung der Risiken und eine konzerneinheitliche Vorgehensweise implementiert. Risiken eines Unternehmens sind dabei Gegenstand einer gesamthaften Sicht. Dabei sollte die Risikostrategie von der Unternehmensstrategie abgeleitet werden, damit eine Detailstrategie zur Erkennung und zum Umgang mit Risiken eingebettet werden kann (vgl. Möbius et al. 2013, S. 48 und S. 50).

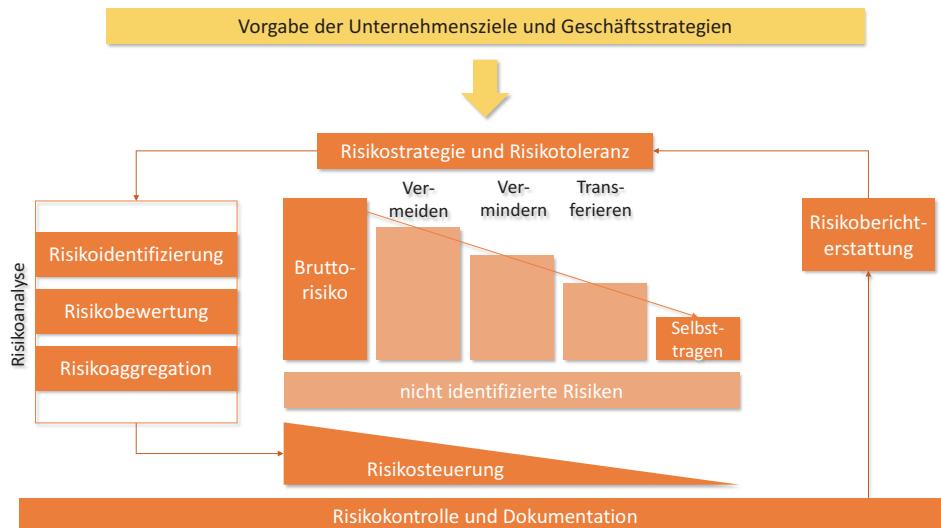


Abb. 14.4 Risikomanagementprozess. (Quelle: eigene Darstellung in Anlehnung an Rohlfs 2018, S. 75)

Konkret muss der Firmenverbundene Vermittler auf Basis der Risikostrategie, die aus der Geschäftstätigkeit des Unternehmens resultierenden Risiken analysieren. Dazu gehören die Identifizierung der Risiken sowie deren Bewertung und schließlich die Risikoaggregation. Das bedeutet der Firmenverbundene Vermittler prüft, welche Risiken in dem Geschäftsmodell und den operativen Tätigkeiten des Industrieunternehmens vorhanden sind und bewertet deren Gefährdungspotenzial für den weiteren Risikomanagementprozess. Anschließend werden die Risiken hinsichtlich ihres Zusammenwirkens und, ob das Unternehmen die Risiken selbst tragen kann und möchte, beurteilt (vgl. Rohlfs 2018, S. 75 f.).

Sollen die Risiken nicht selbst getragen werden, müssen diese gesteuert werden. Dazu gehört die Beurteilung, welche Risiken durch bestimmte Maßnahmen ganz vermieden werden können. Auch können Risiken gemindert werden, zum Beispiel durch Sicherheits- und Kontrollmaßnahmen in den betrieblichen Abläufen. Als weitere Absicherungsmöglichkeit steht der Risikotransfer. Darunter ist unter anderem auch der Versicherungseinkauf zu verstehen (vgl. Rohlfs 2018, S. 256 f.). Der Firmenverbundene Vermittler sorgt in diesem Schritt für die Platzierung der Risiken am Versicherungsmarkt. Hierbei begleitet er das Versicherungsmanagement von dem Suchen eines oder mehrerer geeigneter Industriever sicherer, über die Ausgestaltung und den Abschluss der Versicherung sowie dem weiteren Bestandsmanagement.

Auch die weitere Kontrolle der Risiken gehört dann zum Aufgabengebiet des Firmenverbundenen Vermittlers. Somit hat der Firmenverbundene Vermittler die Aufgabe und Rolle das betriebliche Risikomanagement inklusive dem Versicherungsmanagement zu betreiben.

14.5 Fazit

Zusammenfassend kann festgehalten werden, dass sich Industrieunternehmen in erster Linie mit den in den operativen Tätigkeiten und Geschäftsmodellen vorhandenen Risiken beschäftigen müssen. Schließlich sind in einem großen Industrieunternehmen, welches häufig auch international tätig ist, komplexe Risiken enthalten. Außerdem verschärft sich die Risikosituation durch weitere aktuelle Änderungen der gesetzlichen und umweltbezogenen Rahmenbedingungen. Daher sollte eine Sicherheit durch ein betriebliches Risikomanagement geschaffen werden, um die Unternehmensexistenz zu schützen und die verfolgte Unternehmensstrategie einschließlich der geplanten Ziele erreichen zu können.

Das Risikomanagement und die zugehörige Strategie sollten sich dabei an der Unternehmensstrategie orientieren und sind unternehmensindividuell zu gestalten. In diesem Rahmen ist es sinnvoll, innerhalb eines Risikomanagementprozesses zu beurteilen, welche Risiken in welcher Intensität und in welchem Zusammenspiel zueinander im Unternehmen vorhanden sind. Anschließend muss sich das Unternehmen überlegen, wie es mit diesen Risiken umgehen möchte.

Ein wichtiger Bestandteil des betrieblichen Risikomanagements ist das Versicherungsmanagement als eine Form des Risikotransfers. Dies ist eine Möglichkeit, wie das Unternehmen die Risiken steuern kann. Im Rahmen dessen wird das Unternehmen erst zum Versicherungskunden und auch zum Versicherungsnehmer. Dabei gibt es organisatorisch verschiedene Möglichkeiten, wie das betriebliche Risikomanagement innerhalb oder außerhalb des Unternehmens geregelt werden kann. Hier sollte das Unternehmen individuell eine geeignete Lösung finden. Dabei muss es sich auch im Klaren darüber werden, wie das benötigte Produkt gestaltet sein sollte.

Wichtig ist es, dass das Unternehmen Kriterien aufstellt, nach denen es den geeigneten Industriever sicherer auswählen will. Insbesondere sind gebotene Serviceleistungen des Versicherers neben den weiteren Vertragsbedingungen wie Deckungssummen und Leistungsinhalten ausschlaggebend. Will der Versicherungsnehmer die Auswahl über einen Versicherungsvermittler treffen, sollte dieser die Anforderungen des Unternehmens berücksichtigen.

Eine Möglichkeit das Versicherungsmanagement inklusive dem Versicherungseinkauf zu betreiben, ist der Einsatz eines Firmenverbundenen Vermittlers. Dieser ist wirtschaftlich und rechtlich abhängig von dem Unternehmen. Dadurch besteht einerseits der Vorteil, dass nicht gegen das Provisionsabgabeverbot verstößen wird. Darüber hinaus ist die Kostenstruktur transparenter als bei externen Versicherungsvermittlern. Außerdem kann unternehmensinternes Know-how aufgebaut werden und der Firmenverbundene Vermittler steht ausschließlich in der Interessensphäre des Unternehmens. Ein weiterer wichtiger Vorteil ist, dass der Firmenverbundene Vermittler einen gesamthaften Blick auf das betriebliche Risikomanagement hat. Ein Firmenverbundener Vermittler kann somit einen erheblichen Mehrwert bieten.

Schlussendlich muss der Versicherungsnehmer jedoch den geeigneten Versicherungsvermittler anhand der vorhandenen Risiken auswählen. Bspw. kann es sinnvoll sein, einen Firmenverbundenen Vermittler für das betriebliche Risikomanagement und den hauptsächlichen Versicherungseinkauf zu beschäftigen. Sollen jedoch Risiken versichert werden, für die ein Spezialwissen erforderlich ist, empfiehlt es sich unter Umständen ergänzend einen Versicherungsmakler oder Spezialversicherungsmakler zur Beratung und zum Versicherungseinkauf einzusetzen. Dies muss das Industrieunternehmen unternehmensindividuell und für das jeweilige Risiko entscheiden.

Literatur

- Beenken, M. (2017). *Versicherungsvertrieb: Absatz von Versicherungen durch Versicherer und Vermittler in Theorie und Praxis*. Karlsruhe: Versicherungswirtschaft.
- Berkenkopf, K. (2005). Firmenverbundene Vermittler blühen. [versicherungsmonitor.de](https://versicherungsmonitor.de/2005/11/18/firmenverbundene-vermittler-bluhnen/). Zugegriffen am 22.06.2019.
- Farny, D. (2011). *Versicherungsbetriebslehre* (5. Aufl.). Karlsruhe: Versicherungswirtschaft.
- Mertens. (2019). Versicherungsmanagement in der Industriever sicherung – Make or Buy? Die VersicherungsPraxis 02/2019. https://wiki.gvnw.de/wiki/wiki-detail/?tx_ttnews%5Btt_news%5D=867&cHash=3be4e4cf570a5b16436d38b293ed8735. Zugegriffen am 22.06.2019.
- Mikosch, C. (1991). *Industrie-Versicherungen: ein Leitfaden für nationale und internationale Unternehmen* (1. Aufl.). Wiesbaden: Gabler.
- Mikosch, C. (2005). *Industriever sicherungen: eine Führung durch den Versicherungsdschungel* (2. Aufl.). Wiesbaden: Betriebswirtschaftlicher Verlag Gabler.
- Möbius, C., et al. (2013). *Risikomanagement in Versicherungsunternehmen* (2. Aufl.). Berlin: Springer Gabler.
- Olbrich, R. (2009). Provisionsabgabeverbot – Reichweite und legale Um gehungsmöglichkeiten. *VersicherungsPraxis*, 2009(12), 241.
- Robold, M. O., et al. (2018). *Sachversicherungen für private und gewerbliche Kunden: Fach- und Führungskompetenz für die Assekuranz: Geprüfter Fachwirt für Versicherungen und Finanzen Geprüfte Fachwirtin für Versicherungen und Finanzen* (3. Aufl.). Karlsruhe: Versicherungswirtschaft.
- Rohlf, T. (2018). *Risikomanagement im Versicherungsunternehmen: Identifizierung, Bewertung und Steuerung* (2. Aufl.). Karlsruhe: Versicherungswirtschaft.
- Romeike, F., et al. (2008). *Risikomanagement in Versicherungsunternehmen: Grundlagen, Methoden, Checklisten und Implementierung* (2. Aufl.). Weinheim: WILEYVCH.
- Romeike, F., et al. (2013). *Erfolgsfaktor Risiko-Management 3.0: Methoden, Beispiele, Checklisten; Praxishandbuch für Industrie und Handel* (3. Aufl.). Wiesbaden: Springer Gabler.
- Schawel, C., et al. (2012). *Top 100 Management Tools [Elektronische Ressource]: Das wichtigste Buch eines Managers Von ABC-Analyse bis Zielvereinbarung* (4. Aufl.). Wiesbaden: Gabler.
- Versicherungsjournal.de. (2019). Wiesbadener Vereinigung beschließt eigene Auflösung. [versicherungsjournal.de](https://www.versicherungsjournal.de/medienspiegel-artikel.php?id=7756). Zugegriffen am 22.06.2019.
- Wagner, F. (2018a). Allgemeine Versicherungsbedingungen (AVB). [wirtschaftslexikon.gabler.de](https://wirtschaftslexikon.gabler.de/definition/allgemeine-versicherungsbedingungen-avb-53443/version-276532). Zugegriffen am 22.06.2019.

- Wagner, F. (2018b). Industriaversicherung. wirtschaftslexikon.gabler.de. <https://wirtschaftslexikon.gabler.de/definition/allgemeine-versicherungsbedingungen-avb-53443/version-276532>. Zugegriffen am 22.06.2019.
- Wagner, F. (2018c). Obliegenheiten. wirtschaftslexikon.gabler.de. <https://wirtschaftslexikon.gabler.de/definition/obliegenheiten-44520/version-267828>. Zugegriffen am 22.06.2019.
- Wagner, F. (2018d). Versicherungsnehmer. wirtschaftslexikon.gabler.de. <https://wirtschaftslexikon.gabler.de/definition/versicherungsnehmer-49688/version-272915>. Zugegriffen am 22.06.2019.
- Wagner, F. (2018e). Versicherungsvermittler. wirtschaftslexikon.gabler.de. <https://wirtschaftslexikon.gabler.de/definition/versicherungsvermittler-47393/version-270658>. Zugegriffen am 22.06.2019.
- Winter, G. (2007). *Versicherungsaufsichtsrecht: kritische Betrachtungen* (1. Aufl.). Karlsruhe: Versicherungswirtschaft.

Jörg Maier ist seit 2002 Geschäftsführer des firmenverbundenen Versicherungsvermittlers und Leiter des Bereichs Corporate Insurance der Voith Unternehmensgruppe, mit Sitz in Heidenheim an der Brenz. Nach erfolgreichem Abschluss seines Wirtschaftsstudiums begann er 1988 seine Karriere bei der Voith Assekuranz Vermittlung GmbH, dem firmenverbundenen Vermittler des weltweit agierenden Voith Konzerns. Dort wurden ihm verschiedene Aufgaben in den Bereichen Riskmanagement, Steuerung Internationaler Versicherungsprogramme, Underwriting und Schaden, unter anderem in den Sparten Sach/BU, Haftpflicht, Transport und Technische Versicherungen anvertraut. Jörg Maier ist Mitglied der Delegiertenversammlung und verschiedener Ausschüsse des GVNW, des Versicherungsarbeitskreises des VDA und Gast im Versicherungsarbeitskreis des BDI.

Katharina Faßbender studierte Versicherungswesen mit den Schwerpunkten Bilanzierung von Versicherungsunternehmen, Lebensversicherung und Rückversicherung am Institut für Versicherungswesen der Technischen Hochschule Köln. Währenddessen machte sie das duale Studium im Konzern der Gothaer und hat in diesem Rahmen auch die Ausbildung zur Kauffrau für Versicherungen und Finanzen mit Schwerpunkt Lebensversicherung abgeschlossen. Im Anschluss absolvierte sie am Institut für Versicherungswesen der Technischen Hochschule auch das Masterstudium Risk & Insurance. Als Nebentätigkeit arbeitete sie währenddessen bei der Gothaer Lebensversicherung AG im Bereich Prozesse und Systeme.



Bedeutung und Zukunft des Industriever sicherungsmaklers in Deutschland

15

Mathias Pahl, Mirko Domazet und Juliane Ressel

Zusammenfassung

Der Industriever sicherungsmarkt in Deutschland befindet sich gegenwärtig in Bewegung. Veränderte Marktrahmenbedingungen erhöhen den Wettbewerbsdruck und die sich wandelnde Risikolandschaft bedingt veränderte Erwartungen an die Marktteilnehmer. Dazu gehören mitunter erhöhte Ansprüche an die Serviceleistungen hinsichtlich der Aspekte Transparenz, Einfachheit und Reaktionsschnelligkeit sowie die Unterstützung beim professionellen und antizipativen Umgang mit betrieblichen Risiken. Diese Entwicklungen werden als Anlass genommen, das klassische Dienstleistungsrepertoire des Industriever sicherungsmaklers (IVM) den heutigen Kundenbedürfnissen gegenüberzustellen und ein Anforderungsprofil für seine zukünftige Rolle in der Wertschöpfungskette der Industriever sicherung zu erstellen. Durch eine solche Positionierung im Einklang mit den veränderten Kundenbedürfnissen kann es dem IVM gelingen, seine Rolle als unverzichtbarer Risikopartner in einem sich ändernden Marktumfeld zu erhalten und weiter auszubauen. Diesbezüglich besteht die Notwendigkeit eines ganzheitlichen Ansatzes bei der Risikobeurteilung eines Unternehmens, der den Fokus auf die Kernbereiche Risiko, Kapital und Mensch richtet. Mithilfe quantitativer Risikoberatung, digitaler Plattformen und einer zu schaffenden Risikokultur können Risikopotenziale im Unternehmen frühzeitig identifiziert, transparent gemacht und diesen letztlich mit entsprechenden Handlungs- und Absicherungsalternativen begegnet werden.

M. Pahl (✉) · M. Domazet

Willis Towers Watson, Frankfurt am Main, Deutschland

E-Mail: mathias.pahl@willistowerswatson.com; mirko.domazet@willistowerswatson.com

J. Ressel

TH Köln, Institut für Versicherungswesen, Köln, Deutschland

E-Mail: juliane.ressel@gmx.de

15.1 Einleitende Bemerkungen zur Bedeutung des Maklers im deutschen Industrieverversicherungsmarkt

Deutschland gehört laut aktuellen Studien zu den innovationsstärksten Industrienationen der Welt, jedoch ist der Abstand zur Spitzengruppe im Vergleich zu den Vorjahren gestiegen (vgl. BDI 2018; WEF 2019). Um die internationale Wettbewerbsfähigkeit erhalten und weiter ausbauen zu können, spielt die Industrieverversicherung eine stetig wachsende Rolle. Diese ermöglicht den Unternehmen, die bei der Erfüllung ihrer wirtschaftlichen Ziele seit jeher unter Unsicherheit bezüglich der Entscheidungsfolgen agieren, Risiken zur Minderung der eigenen Risikolage an einen Versicherer zu transferieren. Indessen ist das Umfeld, in dem die Unternehmen agieren, in den letzten Jahren unberechenbarer und komplexer geworden. Damit einhergehend sind auch die Risiken, denen sie sich aussetzen, weiter gestiegen (vgl. AGCS 2020; WEF 2020). Jene alten und neuen Bedrohungen stellen das Risikomanagement der Unternehmen vor zahlreiche Herausforderungen und führen nicht selten zu einer Betriebsunterbrechung oder gar zum Stillstand und damit zu erheblichen finanziellen Verlusten (vgl. Harms 2019; WTW 2019). Angesichts der zunehmenden Komplexität der Risikolandschaft steigt auch die Unsicherheit bei der Analyse der unternehmensspezifischen Risiken; alte Prozesse und Strukturen greifen inzwischen zu kurz. Somit wird es für die Unternehmen immer schwieriger, die eigene Risikosituation richtig einzurordnen und sich angemessen abzusichern. Dabei kann der Industrieverversicherungsmakler (IVM) mit seinem Repertoire an Fähigkeiten und Kompetenzen bezüglich der Risikoanalyse und -steuerung sowie seiner internationalen Marktkenntnisse und Zugänge einen entscheidenden Beitrag leisten. Seine Bedeutung in der Wertschöpfungskette ist dabei substanzial größer als im Privatkundengeschäft wie die Wahl der Vertriebswege illustriert: Während der Anteil von unabhängigen Vermittlern (dies umfasst Makler und Mehrfachvertreter) am Neugeschäft in der gesamten deutschen Schaden- und Unfallversicherung bei rund 30 Prozent liegt (vgl. GDV 2019, S. 13), steht der Maklerkanal mit rund 60 Prozent als dominierender Vertriebsweg in der Industrieverversicherung weit vor dem Direktvertrieb und den Ausschließlichkeitsvertretern (vgl. Mahlow und Stressenreuter 2014, S. 26). Dieser hohe Stellenwert wird unter anderem durch die beidseitigen Informationsasymmetrien zwischen Versicherer und Versicherungsnehmer (VN) bedingt. Einerseits erschwert die starke Produktdifferenzierung der Anbieter aus Kundensicht die Bewertung des eigenen Versicherungsbedarfes, andererseits besitzt der Versicherer keine hinreichenden Informationen über die individuellen Bedürfnisse und das Risikoprofil des VN (vgl. Höckmayr 2012, S. 29 ff.). Indem der IVM als Sachwalter des Kunden die Transparenz im Versicherungsmarkt erhöhen und nachfolgend die Marktmacht der Anbieter reduzieren kann, hat er einen entscheidenden Einfluss auf den Wettbewerb und das Marktgeschehen in der Industrieverversicherung (vgl. Focht 2009, S. 31 ff.). Letzteres unterliegt gegenwärtig einer permanenten Transformation: Sich verändernde Marktrahmenbedingungen erhöhen den Wettbewerbsdruck und die sich dynamisch wandelnde Risikolandschaft bedingt veränderte Erwartungen an die Marktteilnehmer. Um seine Marktposition und Wettbewerbsfähigkeit zu wahren, muss sich der IVM folglich eingehender als je zuvor damit

befassen, wie er seinen Kunden eine mehrwertstiftende Versicherungsdienstleistung anbieten kann.

Die skizzierten Entwicklungen werden daher als Anlass genommen, das klassische Dienstleistungsrepertoire des IVM den heutigen Kundenbedürfnissen gegenüberzustellen und zu fragen, ob und wenn ja, inwiefern daraus ein Anpassungsbedürfnis resultiert. Ausgehend von einer Bestandsaufnahme werden ausgewählte Veränderungstreiber beleuchtet, die sich mit Blick auf die Bedürfnisse der Kundensegmente entsprechend der Unternehmensgröße sowie der sich stetig wandelnden Risikolandschaft erschließen. Daran anschließend wird untersucht, welche Konsequenzen sich für das Dienstleistungsangebot des IVM ergeben. Abschließend werden die im Zuge dieser Analyse gewonnenen Erkenntnisse in einem kurzen Fazit rekapituliert und erste Erfolgsfaktoren abgeleitet.

15.2 Rolle und Aufgabe des Industriever sicherungsmaklers: eine Bestandsaufnahme

Der deutsche Industriever sicherungsmarkt unterscheidet sich in der Praxis insofern deutlich von dem Privatversicherungsmarkt, als standardisierte Produkte aufgrund der vielschichtigen Risikoprofile der großgewerblichen und industriellen Kunden eher die Ausnahme sind. Vielmehr werden die Versicherungsverträge unter Mitwirkung des IVM auf die individuellen Bedürfnisse der VN zugeschnitten.

15.2.1 Rechtliche und wirtschaftliche Betrachtung

Die nachfolgende Einordnung des Versicherungsmaklers aus rechtlicher und wirtschaftlicher Sicht verfolgt das Ziel, ihn von anderen Akteuren des Versicherungsvermittlungsmarktes abgrenzen und zentrale Unterscheidungskriterien offenzulegen.

Position und Funktion des Versicherungsmaklers aus rechtlicher Sicht

Der Versicherungsmakler fällt nach den gesetzlichen Vorgaben des § 59 Abs. 1 VVG unter den Gattungsbegriff der Versicherungsvermittler; sein Pendant ist der Versicherungsvertreter. Diese Begriffsbestimmungen wurden im Zuge der Umsetzung der EU-Vermittlerrichtlinie im Jahr 2007 in das Versicherungsvertragsgesetz (VVG) aufgenommen (vgl. Langheid und Wandt 2016, VVG § 59 Rn. 41). Zu einer Konsolidierung des Versicherungsmaklerrechts führte dabei insbesondere die bedeutende Sachwalterentscheidung des Bundesgerichtshofes (BGH) aus dem Jahr 1985 (vgl. BGH vom 22.05.1985, IVa ZR 190/83): Danach entfernte sich die Rechtsstellung des Versicherungsmaklers insofern von der klassischen Mittlerstellung des Handelsmaklers im Sinne von § 93 HGB, als er nicht neutral zwischen den vertragsschließenden Parteien steht, sondern als treuhänderähnlicher Sachwalter des Kunden in das Lager des VN rückt. Die Legaldefinition in

§ 59 Abs. 3 VVG berücksichtigt diese Entwicklung und konkretisiert die für den Versicherungsmakler charakteristische Positionierung:

§ 59 VVG – Begriffsbestimmungen

(3) Versicherungsmakler im Sinn dieses Gesetzes ist, wer gewerbsmäßig für den Auftraggeber die Vermittlung oder den Abschluss von Versicherungsverträgen übernimmt, ohne von einem Versicherer oder von einem Versicherungsvertreter damit betraut zu sein. (...)

Danach betreibt der Makler das Vermittlergeschäft in Unabhängigkeit von den Versicherern und wird im Kundeninteresse tätig, da der Anstoß für seine Tätigkeit vom Kunden als Auftraggeber ausgeht. Dieser erteilt dem Makler die Vollmacht kraft eines Maklervertrages, der den Umfang der zugewiesenen Vertretungsmacht spezifiziert. Folglich ist er dem Kunden gegenüber im Rahmen eines Dauerschuldverhältnisses verpflichtet, einen den jeweiligen Bedürfnissen entsprechenden passenden Versicherungsschutz zu beschaffen.

Die Position und Funktion des Versicherungsmaklers manifestiert sich mit Blick auf die gegensätzliche Verortung des Versicherungsvertreters: Charakterisiert als „Auge und Ohr“ des Versicherers (vgl. Langheid und Wandt 2016, VVG § 69, Rn. 27) erschließt sich das intensive Näheverhältnis zwischen Versicherer und Vertreter, wonach der Vertreter die Interessen des Versicherers zu wahren hat. Er ist durch eine agenturvertragliche Beziehung mit einem (Einfirmen-) bzw. mit mehreren Versicherungsunternehmen (Mehrfachvertreter) verbunden und damit beauftragt, Versicherungsverträge dieser Gesellschaften an die Kunden zu vermitteln. Er kann somit als „Abschlussshelfer des Versicherers“ (Langheid und Wandt 2016, VVG § 69, Rn. 40) bezeichnet werden. Der Versicherungsmakler hingegen, dessen Alleinstellungsmerkmal im Kontext dieses Beziehungsgefüges die Unabhängigkeit von den Versicherern darstellt, vermittelt ständig für mehrere, konkurrierende Versicherungsunternehmen. Dabei entsteht neben dem Vertragsverhältnis mit dem Kunden (dem Maklervertrag) auch ein vertragsähnlich ausgestaltetes Schuldverhältnis zwischen Versicherer und Makler, das zum Beispiel durch Rahmenabkommen und Courtagevereinbarungen rechtsgeschäftlich verstärkt werden kann (vgl. Langheid und Wandt, VVG § 59, Rn. 43). Demzufolge befindet sich der Makler letztlich in einem „Doppelrechtsverhältnis“ (vgl. BGH vom 19.10.1994, IV ZR 39/94). Dennoch, in Abgrenzung zum Versicherungsvertreter, ist der Makler durch die deutlich stärker und enger ausgestalteten Rechtsbeziehungen zu seinen Kunden in erster Linie deren unabhängiger Sachwalter und damit im Lager der VN positioniert (vgl. Zinnert 2008, S. 80).

Position und Funktion aus wirtschaftlicher Sicht

Die Positionierung des Versicherungsmaklers im Beziehungsgefüge zwischen Versicherer und Kunde kann ebenfalls wirtschaftlich definiert werden: Als „Beschaffungsorgan“ des Kunden (vgl. Farny 2011, S. 750) produziert er Vermittlungsdienstleistungen, die er gegen Vergütung an Versicherungsunternehmen liefert. Zu den Aufgaben des Maklers gehören

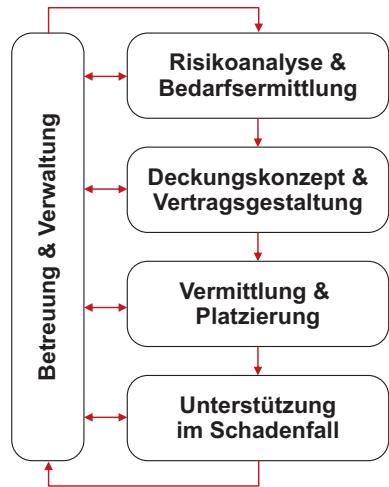
dabei vorrangig eine Reduktion der Transaktionskosten und der Informationsasymmetrien sowie eine Stärkung der Verhandlungsposition (vgl. unter anderem Beenken 2019, S. 36 f.).

Dies bedeutet im Einzelnen, dass der Makler dem VN aufgrund seiner Marktkenntnisse und -zugänge schneller und günstiger ein passendes Produkt vermitteln kann als es diesem in Eigenregie gelingen würde: Er reduziert folglich die Suchkosten für den Kunden (vgl. Griess und Zinnert 1997, S. 33). Unter Suchkosten kann dabei jener zeitliche und finanzielle Aufwand des Kunden verstanden werden, den er zur Informationsbeschaffung, Vertragsvereinbarung und -durchsetzung aufbringen müsste. Diese aus der Transaktionskostentheorie abgeleitete Überlegung des Abbaus der Suchkosten begründet sich durch die im Versicherungsmarkt bestehenden beidseitigen Informationsasymmetrien: Versicherer und VN verfügen nicht über dieselben Informationen hinsichtlich des zu versichernden Risikos (Asymmetrie zugunsten des VN) und der passenden Produkte (Asymmetrie zugunsten des Versicherers). Damit einhergehend fehlt dem VN in der Regel der vollumfängliche Marktüberblick und die Möglichkeit, die Versicherer nach relevanten Kriterien, zum Beispiel der Solvenz, zu bewerten. Der Grad der Intransparenz ist, verstärkt durch die Immateriellität und Komplexität des Versicherungsproduktes, aus Sicht des VN besonders hoch. Im Kontext des Risikotransfers besteht demnach eine Prinzipal-Agenten-Beziehung zwischen Versicherer (Agent) und VN (Prinzipal), die Anreize für opportunistisches Verhalten bietet (vgl. Höckmayr 2012, S. 29). Durch die Beaufragung eines Versicherungsvermittlers entstehen zwei weitere kritische Prinzipal-Agenten-Beziehungen, in denen der Vermittler jeweils als Agent agiert und dessen zwei Prinzipale der VN respektive der Versicherer sind (vgl. Höckmayr 2012, S. 29). Es entsteht folglich ein Spannungsverhältnis, in dem der Vermittler die Interessen beider Prinzipale ausgleichen muss. Im Licht der theoretischen Überlegungen ist es diesbezüglich die Aufgabe des Maklers als Informationsintermediär, die Asymmetrien zu verringern und einen für beide Seiten zielführenden Interessenausgleich und damit eine erfolgreiche Transaktion zu ermöglichen (vgl. Focht 2009, S. 25). Der Prozess der Informationsbeschaffung und -aufbereitung geschieht aufgrund der Positionierung des Maklers als Sachwalter des VN interessenorientiert und ermöglicht so eine Stärkung der Verhandlungsposition des VN (vgl. Griess und Zinnert 1997, S. 33). Dies kann mitunter zu einer innovativen Produktgestaltung oder -entwicklung beitragen, sofern die vom Makler an den Versicherer kommunizierten veränderten Kundenbedürfnisse umgesetzt werden. Diese abstrakt anmutenden Grundfunktionen der Maklertätigkeit lassen sich mit Blick auf das in der Praxis angebotene Dienstleistungsspektrum des IVM im Folgenden konkretisieren.

15.2.2 Klassisches Dienstleistungsrepertoire

Die dienstleistenden Tätigkeiten des IVM werden anhand der Wertschöpfungsprozesse in Abb. 15.1 dargestellt.

Abb. 15.1 Klassisches Dienstleistungsangebot des IVM. (Quelle: eigene Darstellung)



Der IVM berät seine Kunden auf Basis einer umfassenden Risikoanalyse und Bedarfsermittlung. Hierfür wird zunächst die unternehmensweite Risikosituation in Bezug auf die versicherbaren Risiken erfasst und analysiert. Der Versicherungsbedarf wird sodann unter Berücksichtigung der individuellen Risikostrategie und -toleranz ermittelt und dem bereits bestehenden Versicherungsschutz vergleichend gegenübergestellt. Dabei handelt es sich üblicherweise um eine Beratung für die Hauptversicherungszweige der Sach-, Haftpflicht-, Transport- und Unfall- sowie der technischen Versicherungen. Je nach Ausrichtung des IVM können darüber hinaus verschiedene Neben- oder Spezialzweige angeboten werden, wie zum Beispiel die Kfz-Flottenversicherung oder die Directors-and-Officers (D&O)-Versicherung. Diese und weitere Spezialzweige sind jedoch nicht ausschließlich als additive Leistungsangebote zu verstehen. Vielmehr positionieren sich dort auch Spezialmakler, die ihren Fokus explizit auf eine Industrie oder ein bestimmtes Risiko und damit einhergehend ein spezifisches Versicherungsprodukt oder eine Versicherungssparte richten.

Auf dieser Grundlage entwickelt der IVM ein maßgeschneidertes Deckungskonzept, das den bestehenden Versicherungsschutz optimiert. Für dessen Umsetzung fordert er Angebote von geeigneten Risikoträgern an. Eine solche ausgewogene und objektive Marktuntersuchung erfolgt entweder durch eine formale Ausschreibung der Versicherungsleistungen oder durch die gezielte Ansprache vorselektierter Versicherer. Zu den Auswahlkriterien gehören in erster Linie die angebotene Leistung und die Prämie sowie die Solvabilität und der Schadenabwicklungsprozess des Anbieters. Der IVM nimmt dabei unter Einsatz von Fachkompetenz und Kreativität entscheidenden Einfluss auf die Verhandlungen, insbesondere hinsichtlich der Vertragsgestaltung und der Prämien. Die ausgewerteten Angebote werden dem Kunden anschließend in einer Präsentation vorgestellt und erläutert, sodass dieser auf Basis der geschaffenen Entscheidungsgrundlage die für ihn passende Versicherungslösung auswählen kann. Es folgt die preisgerechte Platzierung

und Polierung des mit dem Kunden abgestimmten Deckungskonzeptes bei einem bzw. bei mehreren Versicherern. Letzteres bezieht sich auf Konsortiallösungen bzw. eine Mitversicherung, die insbesondere für die Abdeckung von komplexen Großrisiken relevant ist. Je nach Vereinbarung mit dem Versicherer, übernimmt der IVM dabei die Ausfertigung der Versicherungspolicen oder, sofern die Dokumentierung vonseiten des Versicherers erfolgt, deren Prüfung auf Kongruenz mit den zuvor getroffenen Vereinbarungen. Weitere Tätigkeiten im Rahmen des Vertragsmanagements beziehen sich auf die Prüfung der Prämienrechnungen oder die Durchführung des Inkassos sowie auf notwendige Anpassungen der Versicherungsverträge an veränderte Risiko- und Marktverhältnisse. Dies veranschaulicht die über den Abschlussprozess hinausgehenden fortlaufenden Betreuungs- und Verwaltungsaufgaben des IVM während der Vertragslaufzeit, zu denen ebenfalls die Jahresbesprechungen und die Unterstützung des Kunden im Schadenfall gehören. Letztere reicht von der fristgerechten Schadenemeldung bis zu der abschließenden Verhandlung mit dem Versicherer. Dazwischen begleitet der IVM den Kunden proaktiv während des gesamten Schadenprozesses, zum Beispiel durch die Beratung bei der Auswahl geeigneter Sachverständiger oder die Analyse der Schadendokumentation, und vertritt dessen Interessen gegenüber dem Versicherer im Hinblick auf alle schadenbedingten und ersatzpflichtigen Kosten.

Die klassischen Dienstleistungen des IVM zielen folglich schwerpunktmäßig darauf ab, ausgehend vom Risikoprofil des Kunden die darauf abgestimmten Bedarfe abzuleiten und das entwickelte Deckungskonzept unter fachkundiger Auswahl geeigneter Anbieter am Markt zu platzieren. Der Abschluss eines Versicherungsvertrages zwischen VN und Versicherer löst den Courtageanspruch des Maklers aus, sofern dessen Vermittlertätigkeit für das Zustandekommen ursächlich war (vgl. Griess und Zinnert 1997, S. 155). Dieser Vermittlungserfolg wird im Courtagemodell durch den Versicherer variabel vergütet, das heißt orientiert am vermittelten Prämienumsatz. Neben diesem etablierten Vergütungssystem (mit den konstitutiven Merkmalen der Erfolgsabhängigkeit, Umsatzorientierung und Vergütungsschuldnerrschaft des Versicherers; vgl. Beenken 2019, S. 310 f.) wird derzeit das Honorarmodell als alternative Vergütungsform mit Blick auf das Umsetzungsgesetz der EU-Versicherungsvertriebsrichtlinie (Insurance Distribution Directive, IDD) öffentlichkeitswirksam diskutiert (vgl. unter anderem Deutscher Bundestag 2017, S. 35). Unter Honorar wird dabei eine vom Kunden bzw. VN geschuldete Vergütung des Versicherungsmaklers verstanden, die entweder erfolgs- oder aufwandsabhängig gestaltet sein kann (vgl. Beenken 2019, S. 327). Bislang wurde diese Form der Vergütung in erster Linie mit dem Berufsbild des (Honorar-)Versicherungsberaters verknüpft, der ausschließlich die Beratung hinsichtlich der Vereinbarung, Änderung oder Prüfung von Versicherungsverträgen übernimmt (vgl. § 59 Abs. 4 VVG). Dafür bedarf er infolge der überarbeiteten Gewerbeordnung nicht mehr der Erlaubnis nach § 34e Abs. 1 GewO alte Fassung, sondern fällt fortan unter den Erlaubnistatbestand des § 34d Abs. 2 GewO. Weiterhin ist eine gleichzeitige Tätigkeit als Versicherungsvermittler und als Versicherungsberater nicht zulässig. Im Industriever sicherungsmarkt hat die gegenwärtige Debatte über das Honorarmodell keine tief greifenden Auswirkungen entfaltet, da gemäß § 34 d Abs. 1 S. 4 GewO bereits in der

Vergangenheit eine Honorarvereinbarung zwischen Industrikunden und IVM abgeschlossen werden konnte. Insofern ergeben sich für den IVM keine wesentlichen Änderungen zu den vorherigen Vergütungsregelungen.

15.2.3 Marktüberblick

Im DIHK-Vermittlerregister sind derzeit 198.452 Versicherungsvermittler und -berater eingetragen, von denen 46.286 als Makler tätig sind (Stand: 02.01.2020, vgl. DIHK 2020). Einige davon sind im Bundesverband Deutscher Versicherungsmakler (BDVM) organisiert, der als führender Interessenverband bis dato über 800 Mitgliedsunternehmen mit mehr als 11.000 Mitarbeitern vertritt (vgl. BDVM o. J.). Eine Gruppe dieser Maklerunternehmen sind die IVM, die in Abb. 15.2 auf Basis öffentlich verfügbarer Informationen kategorisiert werden.

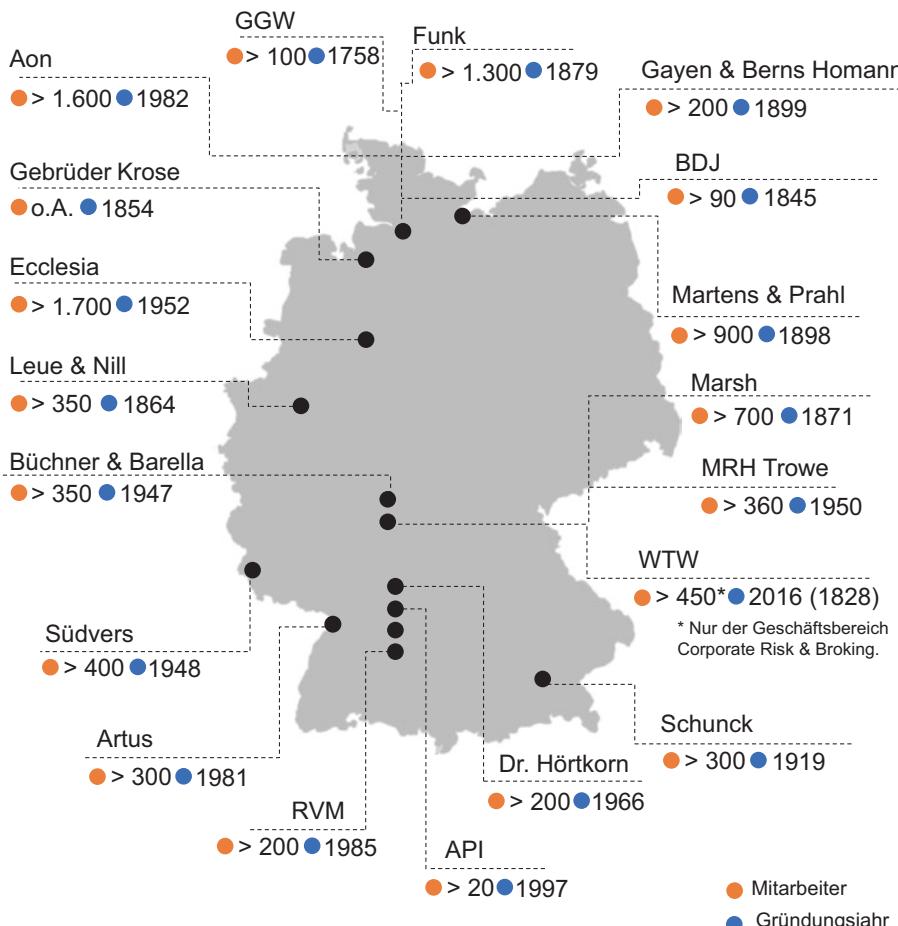


Abb. 15.2 Marktüberblick über IVM in Deutschland. (Quelle: eigene Darstellung)

In Bezug auf die Mitarbeiterzahlen zählt die Ecclesia Gruppe mit rund 1750 Mitarbeitern zu den größten IVM im deutschen Markt, gefolgt von Aon mit ca. 1650 und Funk mit ca. 1320 Mitarbeitern (Stand: Februar 2020). Der Großteil der abgebildeten Unternehmen ist inhabergeführt. Um den Kunden auch eine internationale Betreuung anbieten zu können, kooperieren die Maklerhäuser, die nicht Teil eines globalen Maklerkonzerns sind, mit ausländischen Maklerunternehmen bzw. gehören internationalen Netzwerken, wie zum Beispiel European Brokers Network (Eubronet) oder Assurex Global an.

Abgesehen von der nicht-privaten Sachversicherung liegen bislang nicht ausreichend belastbare Zahlen vor, um das gesamte Prämienvolumen des deutschen Industriever sicherungsmarktes zu ermitteln. Schätzungen verschiedener Studien beziehen sich häufig nur auf abgegrenzte Sparten, so beziffert zum Beispiel Oliver Wyman den Anteil der gewerblichen Kunden an den Beitragseinnahmen in der Schaden- und Unfallversicherung auf 38 Prozent (vgl. Oliver Wyman 2018, S. 2).

15.3 Ausgewählte Entwicklungstendenzen im Industriever sicherungsgeschäft

Angesichts der Tragweite der sich wandelnden gesellschaftlichen, rechtlichen und technologischen Rahmenbedingungen wird das Risikomanagement der VN vielschichtiger und der IVM muss sich mehr als je zuvor damit befassen, inwiefern er Mehrwerte für seine Kunden generieren kann. Aufgrund des steigenden Tempos der dynamischen Entwicklungen kann der nachfolgende Überblick nur als Momentaufnahme verstanden werden, der keinen Anspruch auf Vollständigkeit erhebt. Vielmehr soll ein grundsätzliches Verständnis der Ursachen für die veränderten Anforderungen an den IVM entwickelt werden.

15.3.1 Veränderte Kundenerwartungen und -bedürfnisse

Nachfolgend wird zwischen dem deutschen Mittelstand und den multinationalen Großunternehmen differenziert. Eine solche Abgrenzung ist weder in der Literatur noch in der Praxis einheitlich definiert, sondern soll schematisch dafür sensibilisieren, dass die Kundenwünsche je nach Unternehmensgröße variieren können und eine entsprechende Spezialisierung immer wichtiger wird.

15.3.1.1 Deutscher Mittelstand

Die Unternehmenslandschaft des deutschen Mittelstandes ist zum überwiegenden Teil geprägt durch kleine und mittlere Unternehmen (KMU) aus allen Wirtschaftsbranchen. Diese werden vom Institut für Mittelstandsforschung (IfM) Bonn anhand der quantitativen Kriterien des Jahresumsatzes (weniger als 50 Millionen Euro) und der Beschäftigtenzahl

(weniger als 500 Mitarbeiter) sowie des qualitativen Attributs der Einheit von Eigentum und Leistung definiert (vgl. IfM o. J.). Demnach wurden 2016 rund 3,5 Millionen Unternehmen in Deutschland unter den Begriff der KMU subsumiert (vgl. IfM o. J.). Nicht zuletzt aufgrund der Heterogenität dieser Gruppe können verallgemeinerbare Tendenzen nur bedingt abgeleitet werden, dennoch lassen sich einzelne Aspekte schlaglichtartig hervorheben.

Infolge der Globalisierung und des technischen Fortschritts weisen die Wertschöpfungsketten der deutschen KMU einen zunehmenden Internationalisierungsgrad auf (vgl. Holz und Kranzusch 2015). Unabhängig davon, wo und in welcher Form die KMU international tätig sind, potenzieren sich die Abhängigkeiten und damit einhergehend die Risiken, denen sie sich aussetzen. Die Relevanz branchenspezifischer und individueller Versicherungslösungen im Rahmen internationaler Versicherungsprogramme beschränkt sich heute folglich nicht mehr auf Großunternehmen.

Als weiteres Thema ist Corporate Governance bei den KMU angekommen: Angesichts der Vielzahl der kontinuierlich zu treffenden Entscheidungen sind die Geschäftsführer zunehmend Haftungsgefahren ausgesetzt, da Gesetzesverstöße immer akribischer identifiziert und dokumentiert werden (vgl. WTW 2019, S. 12). Zu den größten Risiken für Führungskräfte zählten dabei zuletzt Cyberangriffe und Datenverlust wie aus der Studie zur Managerhaftung hervorgeht, die jährlich von WTW und Allen & Overy veröffentlicht wird (vgl. WTW und Allen & Overy 2018, S. 5). Infolge der zunehmenden Digitalisierung entwickeln bzw. wandeln sich ferner die Geschäftsmodelle einiger KMU und damit einhergehend verändert sich auch ihr Versicherungsbedarf. Um die Risikoposition des Unternehmens zu optimieren, muss die Risikotransferstrategie demnach auf einer umfassenden Risikoanalyse basieren. In den meisten Fällen verfügen die KMU jedoch nicht über einen hauptberuflichen Risikomanager. Angesichts dessen erschließt sich das Bedürfnis einer schnell zu etablierenden, transparenten Entscheidungsgrundlage, auf deren Basis die KMU ein möglichst kostengünstiges und passgenaues Versicherungsangebot auswählen können. Die Toleranz der Kunden gegenüber Umständlichkeit und Intransparenz sinkt dabei stetig: Sie sind aus anderen Branchen ein überzeugendes Kundenerlebnis gewöhnt und übertragen diese Erwartungen hinsichtlich Einfachheit („Convenience“-Faktor) und Transparenz auch auf die Marktteilnehmer des Industriever sicherungsmarktes. Dies gilt sowohl für die Absicherung der Risiken als auch für einen qualitativ hochwertigen und zügigen Service im Schadenmanagement. Die Anforderungen gehen dabei über die im unmittelbaren Zusammenhang mit dem Versicherungsschutz stehende Abwicklungsleistung hinaus: Es werden wertschaffende Zusatzservices erwartet, wie zum Beispiel eine Krisenberatung bzw. Notfall-Hotline im Schadenfall (vgl. Gothaer 2019). Grundsätzlich wird dabei auf Seiten der Versicherer und Makler ein gewisser Digitalisierungsstandard vorausgesetzt und auch die Nachfrage nach digitalen Kunden- und Schadenportalen nimmt weiter zu (vgl. Marsh und Oliver Wyman 2017). Letztlich wandeln sich somit nicht nur die Absicherungsbedürfnisse, sondern auch die Ansprüche an Service, Erreichbarkeit, Transparenz und Einfachheit steigen.

15.3.1.2 Multinationale Großunternehmen und Konzerne

Multinationale Unternehmen (nachfolgend MNU) zeichnen sich gemäß der OECD-Leitsätze dadurch aus, dass sie in mehreren Ländern niedergelassen sind, wobei die jeweiligen Unternehmensteile so miteinander verbunden sind, dass sie ihre Geschäftstätigkeit entsprechend koordinieren können (vgl. OECD 2011, S. 19 f.). Unter Berücksichtigung der IfM-Mittelstandsdefinition folgt im Umkehrschluss, dass MNU mehr als 500 Mitarbeiter beschäftigen und einen Jahresumsatz von über 50 Millionen Euro erwirtschaften. Im vorliegenden Kontext handelt es sich um Großunternehmen und Konzerne (zum Beispiel DAX- oder MDAX-Unternehmen), die in der Regel über eine eigene Versicherungsabteilung oder einen firmenverbundenen Versicherungsvermittler bzw. Inhouse Broker verfügen. Einige der MNU bedienen sich zur Absicherung firmeninterner Risiken im Rahmen der Selbsttragung auch eines firmeneigenen Versicherungs- oder Rückversicherungsunternehmens (sogenannte Captive). Sofern die MNU einen externen Versicherungsmakler zur Platzierung und Verwaltung ausgewählter Risiken beauftragen, muss dieser folglich eine gewisse Durchsetzungskraft im Markt vorweisen und durch hohes fachliches Know-how einen messbaren Mehrwert für die Kunden generieren können. Expertise, Erreichbarkeit und Reaktionsgeschwindigkeit werden dabei zu den zentralen Treibern für die Kundenzufriedenheit (vgl. Darnell et al. 2018, S. 6 f.). Der Kunde schätzt somit Ansprechpartner, die ihre Branche, ihre Herausforderungen und Ziele verstehen, unabhängig davon, ob es sich um Fragen aus einer speziellen Branche oder um spezifische Produkte handelt.

Bei den MNU stehen folglich die ganzheitliche Beratung und Internationalität im Vordergrund. Dabei erwarten die Kunden vom IVM eine fundierte Kenntnis des Unternehmens, die nicht durch eine isolierte Jahresbesprechung erzielt werden kann, sondern einen fortlaufenden Dialog über das Geschäftsmodell und die entsprechenden Herausforderungen und Risiken erfordert. Dies gilt insbesondere mit Blick auf neuartige, oftmals immaterielle Risiken, wie Lieferkettenunterbrechungen oder Cybervorfälle, die sich schnell verändern und keine gesicherten Schadenerfahrungen aufweisen. Die Interdependenzen, die das Anfälligkeitsrisiko erhöhen, nehmen dabei infolge der globalen Arbeitsteilung, der Automatisierung und der Komplexität der Produktionsprozesse weiter zu. Beispielsweise führen Just-in-time-Konzepte aus Unternehmenssicht zunächst zu einer Senkung der Kosten und einer Steigerung der Effizienz, zugleich resultieren daraus jedoch auch steigende Risiko- und Schadenpotenziale. Folglich zählt die Analyse von Lieferkettenrisiken – große Industrieunternehmen zählen mitunter 10.000 Lieferanten und Sublieferanten weltweit (vgl. Bruch und Münch 2018, S. 68) – und die Quantifizierung der daraus resultierenden Betriebsunterbrechungspotenziale zu den besonders komplexen Risikoanalysen. Die Großindustriekunden brauchen daher einen verlässlichen Partner, der mit ihnen nicht nur Preis- und Konditionsunterschiede verschiedener (bestehender) Versicherungslösungen bespricht. Vielmehr muss gemeinsam analysiert werden, welche Gefahren unterschätzt oder noch gar nicht erkannt wurden und wie das Unternehmen im Branchenvergleich abschneidet, um den Kunden dann bei der Abwägung unterstützen zu können, ob ein Risikotransfer durch Versicherungslösungen wirtschaftlich sinnvoll ist. Letzteres schafft eine

verbindliche Entscheidungsgrundlage zugunsten einer risikobasierten Versicherungsstrategie, die auch die jeweilige Unternehmensstrategie widerspiegelt. Im Einklang mit den komplexen Wertschöpfungsketten der MNU müssen die internationalen Versicherungsprogramme eine weltweite Absicherung der Risiken gewährleisten und zugleich lokale Standards, wie gesetzliche Bestimmungen und steuerrechtliche Vorgaben, erfüllen. Dabei werden die MNU vonseiten interner (zum Beispiel Anteilseigner) wie externer Akteure (zum Beispiel Regulierungsbehörden) mit immer höheren Erwartungen beim professionellen und antizipativen Umgang mit Risiken konfrontiert. Der Bedarf, Risiken zu verstehen, ist daher in den letzten Jahren erheblich gestiegen und damit auch die Anforderung an den IVM, umfangreiche Risikoinformationen so zu erheben und auszuwerten, dass diese in das holistische Risikomanagementsystem eingebettet werden können. Zudem nehmen die kundenseitigen Anforderungen an die Versicherungsprodukte und damit an das Produktmanagement der Versicherer zu. Diesbezüglich müssen Innovationen gefördert und die Grenzen der Versicherbarkeit vonseiten des IVM stetig infrage gestellt werden, um Einfluss auf die Entwicklung neuer bzw. die Weiterentwicklung bestehender Produkte zu nehmen. Ebenfalls lassen sich Veränderungswünsche hinsichtlich des Schadenmanagements konstatieren: Über die technische Schadenabwicklung hinaus soll mittels moderner Technologien, die Echtzeit-Datenströme generieren, die Schadenprävention forciert werden, um potenzielle Schäden frühzeitig abzuwenden. Überdies kann die Modellierung der unternehmensindividuellen versicherbaren Risiken insofern optimiert werden, als die neuen Technologien im Bereich der Schadenabwicklung zu einem verbesserten Verständnis der dahinterliegenden Risiken und damit der Inputdaten führen.

15.3.2 Veränderung der Risikolandschaft

Unternehmen sind seit jeher mit Unsicherheiten und Risiken konfrontiert; deren Ausmaß und Komplexitätsgrad hat sich jedoch erheblich erhöht. Diese Wahrnehmung wird durch verschiedene Studien, wie exemplarisch dem Risk Barometer der Allianz Global Corporate & Specialty (AGCS) oder dem Global Risks Report des World Economic Forum (WEF) unterstrichen (vgl. AGCS 2020; WEF 2020). Vergleicht man die Rankings der letzten Jahre wird zunächst ersichtlich, dass traditionelle Risiken weiterhin als eine große Bedrohung wahrgenommen werden: Sieben Jahre in Folge führten Betriebsunterbrechungen das Allianz Risk Barometer der größten Geschäftsrisiken an (vgl. AGCS 2019, S. 10). In diesem Jahr wurden sie erstmals von Cybervorfällen abgelöst und fielen auf den zweiten Platz (vgl. AGCS 2020, S. 4). Auch die Gefahr von Naturkatastrophen rangiert weiterhin auf den vordersten Plätzen (vgl. AGCS 2020, S. 4; vgl. WEF 2020, S. 28 ff.). Die steigende Anzahl der Großschäden in den vergangenen sieben Jahren mit einer Schadensumme von über 100 Millionen Euro (vgl. Harms 2019) illustriert dabei die Zunahme des Risikopotenzials und -ausmaßes dieser und weiterer klassischer Unternehmensrisiken.

Gleichzeitig prägen neue Bedrohungen den öffentlichen Diskurs und gewinnen maßgeblich an Bedeutung: Hackerangriffe, Datendiebstahl, Ransomware- oder Distributed-

Denial-of-Service-(DDoS)-Attacken, um nur einige Cybervorfälle zu nennen, rücken zunehmend in den Blickpunkt der Unternehmen. Die vielfältigen Ausprägungen illustrieren die großen Herausforderungen im Umgang mit Cyberrisiken, da sich hinter diesem Begriff Gefahren verbergen, die schwer vorhersehbar und deren finanzielle Folgen kaum abzuschätzen sind. Folglich haben Cyberrisiken ihren kontinuierlichen Aufstieg in dem Ranking fortgesetzt (Platz 15 im Jahr 2013) und sind dieses Jahr erstmals als größtes Geschäftsrisiko weltweit eingestuft worden (AGCS 2020, S. 11 ff.). Angesichts der stärkeren Vernetzung der Risiken zählen Cybervorfälle darüber hinaus zu den am meisten gefürchteten Auslösern von Betriebsunterbrechungen (vgl. AGCS 2020, S. 11 ff.). Die Unternehmen müssen folglich mit einer Vielzahl komplexer Auslöser und Szenarien rechnen; eine isolierte Betrachtung der einzelnen Risiken durch funktionale Fachabteilungen greift inzwischen zu kurz. Neben den finanziellen Verlusten aus einer Betriebsunterbrechung stellt gerade im Zeitalter der sozialen Medien auch der Reputationsverlust ein wachsendes Problem dar. Eine Studie von Pentland Analytics und Aon über 125 Reputationskrisen der letzten zehn Jahre ergab, dass sich deren Einfluss auf die Aktienkurse seit der Einführung von sozialen Medien verdoppelt hat (vgl. Pretty 2018, S. 5). Zu den Folgen zählen unter anderem Ertragsausfälle, erhebliche Marketingkosten sowie eine geschwächte Wettbewerbskraft, sofern das Vertrauen der Kunden verloren gegangen ist. In einer zunehmend komplexen Unternehmensumwelt ist es daher notwendig, die Risikopotenziale im Unternehmen frühzeitig zu identifizieren, transparent zu machen und diesen mit entsprechenden Handlungs- und Absicherungsalternativen zu begegnen. Speziell mit Blick auf neuartige Risiken, sogenannte „Emerging Risks“, ergeben sich besonders hohe Anforderungen an das vielschichtige Risikomanagement im Unternehmen: Diese Risiken zeichnen sich mangels vorliegender Erfahrungswerte zu Ursachen und Auswirkungen durch ein hohes Maß an Unsicherheit aus. Dennoch sollte ein Dialog über die zukünftige Risikolandschaft angestoßen werden, um sich auch auf Eventualitäten angemessen vorbereiten zu können.

Im Fokus der Betrachtung stehen zunehmend auch geopolitische und geoökonomische Risiken. Diese haben in den letzten Jahren zu einem deutlichen Anstieg unternehmerischer Verluste geführt und können aufgrund der gegenseitigen Abhängigkeiten zudem die traditionellen Geschäftsrisiken in ihrem Ausmaß noch verstärken (vgl. WEF 2020, S. 10 f.). Exemplarisch seien hierfür gegenwärtige Handelskonflikte, internationale Strafzölle und Wirtschaftssanktionen, Währungskrisen, aber auch nationalistische und populistische Tendenzen in Europa angeführt. Gemäß einer Studie von WTW und Oxford Analytica, dem Political Risk Survey 2019, verzeichnete mehr als die Hälfte der befragten Unternehmen mit einem Umsatz von mehr als einer Milliarde US-Dollar Umsatz in den letzten Jahren Einbuße aufgrund von politischen Risiken (vgl. WTW und Oxford Analytica 2019, S. 6). Zu den drei am häufigsten genannten Gründen zählten Verluste durch politische Gewalt, Beschränkungen des Wechselkurstransfers sowie Import- und Exportembargos (vgl. WTW und Oxford Analytica 2019, S. 6).

Ferner nimmt die Bandbreite der Risiken auch durch globale Trends, wie zunehmende Einkommens- und Vermögensungleichheit, Klimawandel und den technischen Fortschritt weiter zu oder wird durch diese erst verursacht (vgl. WEF 2020, S. 18 ff.). Jene Schlag-

wortliste ließe sich an dieser Stelle noch um ein Vielfaches erweitern. Insgesamt erschließt sich, dass dieser tief greifende Wandel einen erheblichen und vielschichtigen Einfluss auf die Risikolandschaft von Unternehmen aller Industrien und Größenordnung hat. Als Zwischenfazit kann gezeigt werden, dass sich die Unternehmen heute Risiken gegenübersehen, die in den letzten Jahren massiv an Gewicht gewonnen haben und sich immer gravierender auf Wertschöpfungsprozesse und Finanzziele auswirken. Letzteres impliziert, dass die Unternehmensrisiken mehrdimensional und zunehmend verkettet sind und dadurch potenziell größere Auswirkungen haben. Durch die zunehmend verstärkten Interdependenzen in einer digitalisierten Unternehmenswelt stellen neben den gegenwärtigen auch die zukünftigen neuartigen Risiken eine zentrale Herausforderung für das Risikomanagement dar.

15.3.3 Auswirkungen auf das Leistungsangebot des Industrieversicherungsmaklers

In Anknüpfung an die sich dynamisch wandelnde Risikolandschaft muss sich auch der IVM an das gestiegene Tempo anpassen und zielgerichtete Lösungen für die Industrie anbieten, damit sich seine Kunden auf ihre eigentliche Geschäftstätigkeit konzentrieren können. In Anbetracht der unterschiedlichen Facetten der Unternehmensrisiken reichen klassische Standardprodukte dafür nicht mehr aus. Vielmehr werden immer spezifischere Versicherungslösungen benötigt. Die Kunst liegt dabei in der Bewertung der Risiken und der Erstellung eines aussagekräftigen Risikoprofils. Folglich erschließt sich die Notwendigkeit eines ganzheitlichen Ansatzes bei der Risikobeurteilung eines Unternehmens, der die nachfolgenden Aspekte berücksichtigt:

15.3.3.1 Quantitative Risikoberatung und Analyse (Risk Analytics)

Die Relevanz von modernen Methoden des Risikomanagements zur Bewertung und Absicherung von Risiken nimmt weiter zu: Die althergebrachten Ansätze greifen inzwischen zu kurz. Eine professionelle Herangehensweise im Sinne einer systematischen Bewertung und individuellen Quantifizierung von Risiken schafft dabei eine neue und sehr fundierte Grundlage bei der Abwägung, ob ein Risikotransfer durch Versicherungslösungen wirtschaftlich sinnvoll ist. Hierbei muss als Entscheidungskriterium ebenfalls der ökonomische Wert einer Absicherungsstrategie und die Wirkung der Risiken auf Finanzkennzahlen herangezogen werden, um das gesamte Ausmaß beurteilen zu können. Folglich wird eine weitgreifende Datenanalysek Kompetenz in den Anforderungskatalog des IVM Einzug finden, die derzeit vielfach unter dem Begriff „Risk Analytics“ diskutiert wird. Darunter fallen in erster Linie die nachfolgenden vier Anwendungsbereiche.

Erstens, im Hinblick auf den Beginn des Wertschöpfungsprozesses, können im Rahmen der Risikoidentifizierung und -bewertung moderne Software-Tools eingesetzt werden, welche die Risiken stochastisch identifizieren und modellieren können. Eine solche Verarbeitung größerer Datensätze ermöglicht die transparente Auswertung des indivi-

duellen Risikoprofils des Kunden und darauf aufbauend die Entwicklung von Benchmarks und Referenzkategorien. Derzeit kommt dies vorrangig zur Anwendung bei der Naturkatastrophenmodellierung sowie für D&O- und Cyberrisiken. Die potenzielle Vorgehensweise solcher Software-Tools kann überblicksartig wie folgt dargestellt werden: Im Rahmen der Prognose der ausgewählten Unternehmensrisiken bewertet ein Programm das gesamte individuelle Schadenspotenzial und bietet strategische Entscheidungshilfen zur Optimierung der Risikotransferlösungen im Einklang mit der eigenen Risikotoleranz. Bei der Modellierung können unternehmensspezifische oder allgemeine Szenarien betrachtet und über Branchen- sowie Ländergrenzen hinaus hinsichtlich ihrer erwarteten Häufigkeit und dem Schadensausmaß mit auswählbaren Peers, zum Beispiel aus der gleichen Branche oder dem gleichen Aktienindex, verglichen werden. Ein weiteres Einsatzgebiet moderner Software-Tools ist die Unterstützung des Kunden bei der Ermittlung seiner persönlichen Risikotoleranz (Risikoappetit) durch sogenannte Risikomanagement-Tools. Dies kann neben einer grundsätzlichen Analyse der Risikotragfähigkeit, eine Darstellung der möglichen Veränderungen der wichtigsten Finanzkennzahlen in vorgegebenen Schadensfällen und möglicherweise auch einen Vergleich dieser Finanzkennzahlen mit auswählbaren Peers aus unterschiedlichen Unternehmen umfassen, um die eigene finanzielle Widerstandsfähigkeit („Financial Resilience“) hinsichtlich eingegangener Risiken besser verstehen zu können. Indem mittels moderner Technologien die Schadensszenarien in ihrer Komplexität und ihren Konsequenzen angemessen quantifiziert und diese mit der individuell ermittelten Risikotoleranz verglichen werden, erhalten die Unternehmen die Möglichkeit, ihre Entscheidung über Mitigation, Eigentragung oder den Transfer des individuellen Risikos faktenbasiert zu treffen.

Zweitens wird die Eingrenzung auf versicherbare Risiken im Sinne einer ganzheitlichen Risikomanagement-Beratung dahingehend aufgelöst, dass auch nicht versicherbare Risiken, wie zum Beispiel operationelle, strategische und finanzielle Risiken, analysiert werden. Dabei ermöglichen vom IVM durchgeführte „Risk Mapping“-Projekte die Erstellung eines unternehmensindividuellen, weltweiten Risikorankings bei dem die Risikoeintrittswahrscheinlichkeit mit dem Schadenpotenzial im Falle der Risikorealisierung zu einem sogenannten „Gross-Risk Score“ gewichtet werden. Erreicht wird dies durch qualitative Methoden, wie der Befragung relevanter Führungskräfte hinsichtlich ihrer Risikowahrnehmung, oder durch quantitative Modellierungen, wie zum Beispiel der Quantifizierung der Risikoreduzierung nach Umsetzung vorgeschlagener Maßnahmen zur Risikomitigation. Die integrierte Analyse der individuellen Risikotreiber hilft den Unternehmen zusätzlich ihre ganzheitliche Risikolage besser zu verstehen, um entsprechende Schlussfolgerungen für das eigene Risikomanagement treffen zu können.

Drittens werden im Sinne einer technischen Risikoberatung und -steuerung umsetzbare technische Maßnahmen zur Risikominimierung konzipiert, zum Beispiel unternehmensindividuelle Brandschutzkonzepte.

Viertens, mit Blick auf die Risikosteuerung (insbesondere von bisher nicht versicherbaren Risiken) werden Techniken des Alternative Risk Transfer (ART) eingesetzt, um Risiken außerhalb des Erstversicherungsmarktes, zum Beispiel auf den Kapitalmarkt mit-

tels sogenannter „Insurance Linked Securities“ (Versicherungsverbriefungen), zu transferieren. Der größte Teil aller Versicherungsverbriefungen entfällt auf Katastrophenanleihen, sogenannte Cat Bonds (vgl. Liebwein 2018, S. 505 ff.). Die Modellierung des verbrieften NatCat-Exposures erfolgt unter anderem mittels der oben skizzierten Software-Tools. Die zunehmende Datenverfügbarkeit und die neuen Analysemethoden führen überdies zu einer Verbreitung und Weiterentwicklung parametrischer Versicherungslösungen, deren Entschädigungsleistung aus dem Vertrag dann fällig wird, wenn der zu Beginn festgelegte parametrische Referenzwert (zum Beispiel die Windgeschwindigkeit eines Sturms oder die Magnitude eines Erdbebens) einen bestimmten Schwellenwert überschreitet (vgl. Liebwein 2018, S. 516 ff.). Die Risikovolatilität im Zusammenhang mit komplexen Ereignissen wie Naturgefahren kann somit besser erfasst und darauf aufbauend können maßgeschneiderte Transferlösungen abgeleitet werden.

Eine solche Ausweitung des Aufgabenfeldes des IVM bedingt eine Synthese seiner Versicherungs-, Finanzierungs- und Finanzmarktkenntnisse. Zusammenfassend lässt sich hierbei festhalten, dass die originäre Beratungsleistung des IVM durch diese umfangreichen Datenanalyse- und Interpretationskompetenzen weiter gestärkt werden. Dies ermöglicht wiederum die Entwicklung ganzheitlicher und maßgeschneiderter Absicherungsprogramme für den Kunden.

15.3.3.2 Digitale Portale und Anwendungen

Die Digitalisierung ist längst der beherrschende Makrotrend der Versicherungsbranche, entsprechend gilt dies auch für das Industriever sicherungsgeschäft (vgl. Marsh und Oliver Wyman 2017). Doch von einem Primat der Technologie und ihrer Veränderungskraft per se auszugehen, greift hier eindeutig zu kurz. Es sind vielmehr die daraus resultierenden neuen Gestaltungsspielräume, die Potenziale zur Umsetzung der erhöhten Kundenerwartungen an Einfachheit, Reaktionsgeschwindigkeit und Transparenz ermöglichen können. Letzteres kann unter anderem durch den Einsatz von digitalen Plattformen und Anwendungen erhöht werden. Diese bieten dem VN eine übersichtliche Darstellung seiner weltweiten Versicherungsdaten sowie aller versicherungsrelevanten Compliance-Anforderungen. Solche Kundenportale müssen durch eine anwenderfreundliche Oberfläche und Benutzerführung überzeugen und neben der Überblicksfunktion auch einen Zugriff auf die entsprechenden vertrags- und schadenspezifischen Dokumente gewährleisten. Durch den zielgerichteten Einsatz digitaler Anwendungen, speziell im KMU-Bereich, kann der IVM seine Prozesse und Strukturen so anpassen, dass er seine Leistungen weiterhin kostengünstig anbieten kann. Solche Kundenportale sollten dem VN als digitale Informations- und Datenmanagement-Plattform dienen, auf der er eine Online-Schadenmeldung einreichen und dessen Status verfolgen, sich im kuratierten Newsfeed über aktuelle Themen und Nachrichten informieren und mittels des Kontaktmanagements und des gemeinsamen Kalenders Informationen auf kollaborative Weise mit mehreren Benutzern weltweit teilen kann. Letzteres ist insbesondere mit Blick auf auslaufende Verträge und anstehende Vertragsverlängerungen hilfreich und optimiert die Interaktion und den Informationsfluss zwischen Kunde, IVM und Versicherer. Die Kundenschnittstelle kann folglich durch den

Einsatz digitaler Anwendungen neu gestaltet werden. Allerdings bedarf es dafür eines Digitalisierungsverständnisses, das über Automatisierung und Standardisierung hinausgeht und die hochgradig individualisierten Lösungen in der Industriever sicherung angemessen berücksichtigt.

15.3.3.3 Faktor „Mensch“

Eine weitere Notwendigkeit ist die, den Fokus nicht nur auf die zu versichernden Vermögenswerte zu legen, sondern auch den Faktor „Mensch“ in die Beurteilung einzubeziehen, denn die Themen „Risiken“ und „Menschen“ sind eng miteinander verknüpft. Bei einem ganzheitlichen Risikomanagement kommt es daher nicht nur auf analytische Methoden, Datenmengen und IT-Lösungen an, sondern auch darauf, dass die Menschen die Risiken verstehen und angemessen mit ihnen umgehen können. Letzteres beschränkt sich nicht auf die Führungsebene, sondern gilt für jeden einzelnen Mitarbeiter. Exemplarisch kann dies anhand der immer professioneller werdenden Cyberkriminalität illustriert werden, die mittels Phishing-Mails oder Social Engineering vermehrt auf den einzelnen Mitarbeiter als potenzielle Schwachstelle ausgerichtet ist. Durch die sogenannte Fake-President-Attacke auf Unternehmen (Betrüger geben sich dabei als Führungskräfte aus und fordern einen Mitarbeiter per E-Mail oder telefonisch dazu auf bzw. setzen ihn so lange unter Druck, bis er dringende Zahlungen auf angegebene Konten überweist) wurde in den Jahren 2016 und 2017 laut GDV über 150 Millionen Euro erbeutet (vgl. GDV 2018). Die Zahl der Cyberangriffe steigt dabei stetig und betrifft sowohl große als auch mittelständische Unternehmen (vgl. GDV 2018). Angesichts der Professionalität, mit der die Täter vorgehen, bedarf es spezifischer Trainings für die Mitarbeiter sowie einer unternehmensweiten Risikokultur, die das Denken und Handeln der Mitarbeiter weg von dem blinden Ausführen von Aufträgen hin zu einem sensiblen Umgang mit relevanten Risiken ausrichtet. Dies stärkt letztlich sowohl die Resilienz des Unternehmens als auch das Vertrauen der Mitarbeiter und der Kunden und bietet damit auch aus wirtschaftlicher Sicht entscheidende Wachstumschancen.

Um sich noch stärker vom Wettbewerb zu differenzieren, muss sich der IVM auch mit potenziellen Formen der Spezialisierung, zum Beispiel auf eine Industrie oder ein Produkt, bzw. der Segmentierung des Portfolios auseinandersetzen. Letzteres darf sich jedoch nicht auf den originären Leistungsschwerpunkt der Platzierung beschränken, sondern muss das gesamte Dienstleistungsspektrum umfassen und durchgängig an den Kundenbedürfnissen ausgerichtet werden. Im Fokus steht somit immer der Nutzen für den Kunden und ein systematisches Betreuungsmodell, das sich an dessen unternehmerischen Zielen und der Wertschöpfung orientiert. Für einen solchen Wettbewerbsvorteil reicht ein reines Lippenbekenntnis jedoch nicht aus: Es müssen kundenspezifische Alleinstellungsmerkmale entwickelt werden, damit die Kundenerfahrung nachhaltig wertschöpfend ausfällt. Der IVM wird damit zum Problemlöser bei Fragestellungen zu Risiko, Kapital und Mensch, der über den Tellerrand hinausschaut. Dies kann nur durch eine Form der Spezialisierung als Grundlage gelingen.

15.4 Vom Makler zum Risikopartner: ein Ausblick

Die dargestellten Veränderungstreiber bewirken einen profunden Wandel der Versicherungswirtschaft im Allgemeinen und des Berufsstandes des IVM im Speziellen. Seine Kernaufgaben werden sich nachhaltig ändern: Zukünftig muss dem Kunden ein ganzheitlicher Ansatz geboten werden. Es reicht dabei nicht mehr aus, getreu dem Grundsatz „cheap insurance beats everything“ am günstigsten zu offerieren. Vielmehr muss der Fokus auf die Kernbereiche Risiko, Kapital und Mensch gerichtet werden: Der technische IVM wandelt sich so zum Risikopartner und -berater. Letzteres umfasst eine Vielzahl von Bereichen von der quantitativen Risikoanalyse über die Mitarbeiterentwicklung und das Datenmanagement bis hin zum individuellen Risikotransfer. Das Aufgabenspektrum erweitert sich dahingehend, dass der IVM den Kunden dabei unterstützt, die eigene betriebliche Risikolage richtig zu verstehen. Wie eingangs skizziert, wird es für die Unternehmen immer schwieriger, unternehmerische Entscheidungen zu treffen. Die Risiken und Herausforderungen, aber auch die Chancen werden immer komplexer. Somit benötigen die Unternehmen keinen Verkäufer, sondern einen Begleiter und Partner, der das Denken in ganzheitlichen Risikoszenarien forciert und die Transparenz und Verständlichkeit potenzieller Versicherungslösungen erhöht. Dies impliziert eine neue Herangehensweise an die Risiken und damit einhergehend den Einsatz optimierter Analysemethoden zur Risiko-Identifizierung und -bewertung, um dem Kunden eine fundierte Entscheidungsgrundlage zu bieten, welche Risiken (auch ökonomisch betrachtet) transferiert werden sollten. Das aktive Risikomanagement rückt somit stärker in den Fokus und wird sowohl für die MNU als auch für die KMU immer mehr zum Wettbewerbsvorteil. Indem die Unternehmen ihre strategischen Initiativen auf ein solides Fundament stellen können, gewinnen sie an unternehmerischem Freiraum und internationaler Wettbewerbsfähigkeit.

Die Nachfrage nach Beratung und Risikoanalyse wird gerade vor dem Hintergrund der sich dynamisch wandelnden Risikolandschaft auch hinsichtlich nicht versicherbarer Risiken zunehmen und einen Wettbewerbsvorteil für diejenigen IVM generieren, die sich in der Rolle des „trusted advisor“ des Kunden positionieren. Da der Aufbau eines solchen Vertrauensverhältnisses stets mit der gemachten Kundenerfahrung korreliert, muss der IVM mit hoher Expertise überzeugen, transparent kommunizieren und für den Kunden eine solide Entscheidungsgrundlage und damit einen messbaren Nutzen schaffen. Hierfür ist es unerlässlich, sich eingehend mit dem Geschäftsmodell und den spezifischen Risiken der Kunden auseinanderzusetzen, um sie bei der Entwicklung und Gestaltung ihrer jeweiligen Risikostrategie mehrwertstiftend zu unterstützen und eine auf ihre Bedürfnisse zugeschnittene Versicherungs- wie Risikomanagement-Dienstleistung anbieten zu können. Dies impliziert zugleich die zunehmende Relevanz der Spezialisierung und Segmentierung: Aufgrund der unterschiedlichen Kundenbedürfnisse entsprechend der jeweiligen Unternehmensgröße variiert das Verständnis von Versicherungen und damit auch der Anspruch an den IVM. Für die MNU ist unter anderem die Wirkung der Risiken auf die Finanzkennzahlen und -ziele besonders relevant. Dabei ist entscheidend, welchen maximalen

Schaden sich das Unternehmen in einem Jahr in Prozentsatz des Gewinnes vor Zinsen und Steuern ohne weitreichende negative Konsequenzen leisten und wie dieser angemessen auf die zu quantifizierenden Hauptrisiken verteilt werden kann. Der Wettbewerbsdruck für den IVM ist in diesem Segment aufgrund der Inhouse Broker als weitere Akteure besonders hoch. Indem sich der IVM über die transaktionselle Vermittlung von Versicherungsdienstleistungen hinaus Expertise in der Risikomanagement-Beratung aneignet, kann er auch für die Inhouse-Broker der MNU zentrale Mehrwerte generieren. Mit Blick auf das Risikomanagement der KMU müssen sie dazu in die Lage versetzt werden, die Risiken – auch in ihrer Wechselwirkung – mit einheitlichen Methoden bewerten und deren Auswirkungen systematisch transparent machen zu können. Sobald der IVM den eigenen Wettbewerbsvorteil im Zugang und der Betreuung der ausgewählten Kundengruppe benennen und vermitteln kann, kann die Zusammenarbeit zwischen Industrie und Makler maßgeblich verbessert werden. Dafür muss sich sein Leistungsangebot stets im Kontext der sich wandelnden Kundenbedürfnisse messen lassen. Eine der zentralen Herausforderungen für den IVM ist dabei der aktuelle Arbeitsmarkt. Das Problem des Fachkräftemangels führt zu einem „War for Talents“, weshalb es für den IVM immanent wichtig ist, hervorragende Mitarbeiter zu finden und langfristig an sich zu binden sowie junge Talente für die Branche zu begeistern.

Die Implementierung digitaler Technologien verändert sukzessive auch das Risikomanagement der VN. Angesichts dessen bieten die Beschaffung und Nutzung von neuen Daten für den IVM insofern eine weitere Chance zur Differenzierung im Wettbewerb, als ein vertiefter Risikodialog mit dem Kunden geführt und darauf aufbauend ein Deckungskonzept angeboten werden kann, das viel präziser auf das spezifische Risikoprofil des Kunden zugeschnitten ist. Dynamische Risikoinformationen, die zum Beispiel durch festinstallierte Sensoren in Maschinen und Gebäuden im Gegensatz zu den jährlichen Fragebögen in Echtzeit erhoben werden können, können in Kombination mit dem fachlichen Know-how und der Erfahrung des IVM zu einem zunehmend verbesserten Kundenrisikoverständnis beitragen. Dadurch können wiederum die Entscheidungsprozesse auf Seiten des Kunden entscheidend optimiert werden. Für den IVM bedeutet dies, dass er seine Datenanalysefähigkeiten erweitern und die gestiegene Übertragungsfrequenz der neuen Daten in eine dynamische Risikobetrachtung überführen muss. Der gesamte Risikoberatungsprozess muss dabei für den Kunden transparent dargestellt werden, denn ein positives Kundenerlebnis wird auch in der Industriever sicherung zunehmend zum Wettbewerbsfaktor. Aufbauend auf den klassischen Leistungsschwerpunkten ermöglicht eine Verlagerung und Ausdehnung in Richtung der Risikomanagement-Beratung, dass der IVM einen messbaren Mehrwert für seine Kunden generieren kann: Die Risikopotenziale im Unternehmen können frühzeitig erkannt, transparent gemacht und mit entsprechenden Handlungs- und Absicherungsalternativen begegnet werden. Dies kann nur auf der Grundlage eines ganzheitlichen Konzeptes mit einem Fokus auf den Aspekte Risiko, Kapital und Mensch gelingen.

Literatur

- Allianz Global Corporate & Speciality (AGCS). (2019). Allianz Risk Barometer. Top Business Risks for 2019. <https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf>. Zugegriffen am 15.05.2019.
- Allianz Global Corporate & Speciality (AGCS). (2020). Allianz Risk Barometer. Identifying the major business risks for 2020. <https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2020.pdf>. Zugegriffen am 12.02.2020.
- Beenken, M. (2019). *Versicherungsvertrieb: Absatz von Versicherungen durch Versicherer und Vermittler in Theorie und Praxis*. Karlsruhe: Versicherungswirtschaft GmbH.
- Bruch, M., & Münch, V. (2018). Neue Risiken – neues Underwriting. In A. Eckstein, A. Funk-Münchmeyer & A. Liebetrau (Hrsg.), *Insurance & Innovation 2018* (S. 63–71). Karlsruhe: Versicherungswirtschaft GmbH.
- Bundesverband der Deutschen Industrie e. V. (BDI). (2018). Innovationsindikator 2018. <http://www.innovationsindikator.de/2018/>. Zugegriffen am 19.05.2019.
- Bundesverband Deutscher Versicherungsmakler e. V. (BDVM) (o. J.). Viele gute Gründe sprechen für eine Mitgliedschaft im BDVM. <https://bdvm.de>. Zugegriffen am 17.05.2019.
- Darnell, D., Jamnadas, P., & Almquist, E. (2018). *Uncovering the elements of value in commercial insurance*. Bain & Company. https://www.bain.com/contentassets/c2975c96b50c4fc78bd93324defa924a/bain_brief_uncovering_the_elements_of_value_in_commercial_insurance.pdf. Zugegriffen am 23.05.2019.
- Deutscher Bundestag. (2017). Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/97 des Europäischen Parlaments und des Rates vom 20. Januar 2016 über Versicherungsvertrieb und zur Änderung des Außenwirtschaftsgesetzes. <http://dip21.bundestag.de/dip21/btd/18/116/1811627.pdf>. Zugegriffen am 15.05.2019.
- Deutscher Industrie- und Handelskammertag (DIHK). (2020). Registrierungen im Versicherungsvermittlerregister. Stand: 02.01.2020. <https://www.dihk.de/resource/blob/16960/40e6a1ff1ece10a712de33e6cdd488e7/statistik-versicherungsvermittler-januar-2020-data.pdf>. Zugegriffen am 12.02.2020.
- Farny, D. (2011). *Versicherungsbetriebslehre (5. überarbeitete Auflage)*. Karlsruhe: Versicherungswirtschaft GmbH.
- Focht, U. (2009). *Einfluss von Maklern und Wettbewerb auf Industriever sicherungsmärkten. Eine Analyse unter besonderer Berücksichtigung von Vergütungssystemen, Marktstrukturen und Kollusionsanreizen*. Karlsruhe: Versicherungswirtschaft GmbH.
- Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GDV). (2018). Fake-President-Masche: Kriminelle erbeuten mehr als 150 Millionen Euro. <https://www.gdv.de/de/medien/aktuell/fake-president-masche%2D%2Dkriminelle-erbeuten-mehr-als-150-millionen-euro-33240>. Zugegriffen am 19.07.2019.
- Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GDV). (2019). Statistisches Taschenbuch der Versicherungswirtschaft 2019. <https://www.gdv.de/resource/blob/50214/29985281b05d0ce23240d7b7bdff57cd/download%2D%2Dstatistisches-taschenbuch-2019-data.pdf>. Zugegriffen am 22.08.2019.
- Gothaer. (2019). Gothaer KMU Studie 2019 Teil 1: Angst vor Cyber-Angriffen steigt weiter. <https://www.gothaer.de/ueber-uns/presse/publikationen/studien/kmu-studie-2019.htm>. Zugegriffen am 28.06.2019.

- Griess, H., & Zinnert, M. (1997). *Der Versicherungsmakler. Position und Funktion aus rechtlicher und wirtschaftlicher Sicht* (3. Aufl.). Karlsruhe: Versicherungswirtschaft GmbH.
- Harms, W. (2019). Alles steht still. Wie sich Unternehmen gegen Betriebsunterbrechungen absichern können. *Positionen Magazin*, 2019(1), 36–37.
- Höckmayr, G. (2012). *Wandel der Beratungsqualität auf dem Versicherungsvermittlungsmarkt. Eine ökonomische Analyse der Veränderungen aufgrund der Anforderungen der EU-Vermittlerrichtlinie*. Karlsruhe: Versicherungswirtschaft GmbH.
- Holz, M., & Kranzsch, P. (2015). Internationalisierung und Mittelstand, IfM Bonn (Hrsg.), Denkpapier 01/15, Bonn.
- Institut für Mittelstandsforschung (ifM) Bonn. (o. J.). Mittelstandsdefinition des IfM Bonn. <https://www.ifm-bonn.org/definitionen/mittelstandsdefinition-des-ifm-bonn/>. Zugegriffen am 23.05.2019.
- Langheid, T., & Wandt, M. (2016). *Münchener Kommentar zum Versicherungsvertragsgesetz: VVG, Band 1: §§ 1–99, VVG-InfoV* (2. Aufl.). München: C.H.Beck.
- Liebwein, P. (2018). *Klassische und moderne Formen der Rückversicherung* (3. Aufl.). Karlsruhe: Versicherungswirtschaft GmbH.
- Mahlow, N., & Stressenreuter, B. (2014). Know-how-Anforderungen steigen. Wettbewerb und Internationalisierungstendenzen prägen die Industrie-Vertriebslandschaft von 2020. Versicherungswirtschaft Nr. 9 (S. 24–27).
- Marsh und Oliver Wyman. (2017). State of Play – Digitalisierung in der deutschen Industriever sicherung. <https://www.oliverwyman.de/our-expertise/insights/2017/nov/state-of-play.html>. Zugegriffen am 15.05.2019.
- Oliver Wyman. (2018). The Underwriter of the Future. Perspektiven für den Firmen- und Industriever sicherungsmarkt von morgen. <https://www.oliverwyman.de/our-expertise/insights/2018/apr-the-underwriter-of-the-future.html>. Zugegriffen am 23.05.2019.
- Organisation for Economic Co-operation and Development (OECD). (2011). OECD Guidelines for Multinational Enterprises – 2011 Edition. <https://www.oecd.org/corporate/mne/48004323.pdf>. Zugegriffen am 23.05.2019.
- Pretty, D. (2018). Reputation Risk in the Cyber Age – The Impact on Shareholder Value. <https://www.aon.com/reputation-risk-cyber-social-media-pentland-analytics-aon/index.html>. Zugegrif fen am 23.05.2019.
- Willis Towers Watson (WTW). (2019). Industriever sicherungen MARKTspot 2019. https://www.willistowerswatson.com/-/media/WTW/Insights/2019/06/MARKTspot-2019_FINAL.pdf. Zugegriffen am 28.06.2019.
- Willis Towers Watson (WTW) und Allen & Overy. (2018). Directors' liability – D&O: Personal Exposure to Global Risk. http://www.allenovery.com/SiteCollectionDocuments/Directors%20liability_DO%20Personal%20Exposure%20to%20Global%20Risk.pdf. Zugegriffen am 05.06.2019.
- Willis Towers Watson (WTW) und Oxford Analytica. (2019). How are leading companies managing today's political risks? 2019 Survey and Report. <https://www.willistowerswatson.com/en-US/Insights/2019/12/2019-political-risk-survey-report>. Zugegriffen am 12.02.2020.
- World Economic Forum (WEF). (2019). The Global Competitiveness Report 2019. http://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf. Zugegriffen am 12.02.2020.
- World Economic Forum (WEF). (2020). The Global Risks Report 2020 15th Edition. http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf. Zugegriffen am 12.02.2020.
- Zinnert, M. (2008). *Recht und Praxis des Versicherungsmaklers*. Karlsruhe: Versicherungswirtschaft GmbH.

Mathias Pahl studierte nach seiner Ausbildung bei der Deutschen Bank AG in Hamburg Wirtschaftswissenschaften an der Ruhr Universität in Bochum. Er begann seine Karriere 1995 bei Jauch & Hübener zuerst als Trainee, fungierte im Anschluss als Account Director für Großkunden und leitete zum Schluss den Reverse Flow Business Bereich. 2003 wechselte Mathias Pahl zu Willis in der Funktion als Network Country Manager und übernahm die Verantwortung für das Key Account Team in Köln. Ab Januar 2006 fungierte er darüber hinaus als Leiter der Kölner Niederlassung. Im Januar 2007 übernahm er die Funktion als Regional Manager Süd und wechselte in die Niederlassung München. 2009 wurde er CEO von Willis GmbH & Co. KG, Frankfurt, Germany. Im Anschluss an den Merger mit Towers Watson GmbH firmierte sich das Unternehmen um zur Willis Towers Watson Versicherungsmakler GmbH. Mathias Pahl wurde in seiner Rolle Mitglied des deutschen Leadership Teams von Willis Towers Watson und verantwortet das Segment Corporate Risk & Broking.

Mirko Domazet studierte Financial Advisory an der Fachhochschule der Wirtschaft in Verbindung mit einer Ausbildung zum Kaufmann für Versicherungen und Finanzen bei der Deutschen Vermögensberatung AG. Seine berufliche Laufbahn begann er im Jahr 2012 als Vermögensberater, gefolgt von einer Tätigkeit als selbständiger Versicherungs- und Finanzmakler. In 2016 startete Herr Domazet ein Studium als Master of Science in Insurance and Finance, gefolgt von einer Weiterbildung zum Fellow of the Chartered Insurance Institute in London (FCII). Seit 2017 ist er als Referent der Geschäftsleitung bei Willis Towers Watson tätig. In diesem Kontext konnte er sich intensiv mit dem Themengebiet Risk & Analytics sowie der strategischen Kundenbetreuung globaler Unternehmen beschäftigen.

Juliane Ressel studierte Sociology, Politics and Economics mit den Schwerpunkten Risk Management und Leadership an der Zeppelin Universität in Friedrichshafen. Dann arbeitete sie in London bei dem Lloyd's-Versicherungsmakler Butcher, Robinson and Staples und absolvierte im Anschluss das Masterstudium Risk & Insurance am Institut für Versicherungswesen der Technischen Hochschule Köln.



Industriever sicherer im Marktumfeld der Industriever sicherung

16

Christopher Lohmann, Stefan Sowietzki und Pauline Gewand

Zusammenfassung

Die Risikolandschaft für Unternehmen befindet sich in ständigem Wandel. Hierdurch bedarf es einer entsprechenden Anpassung der Industriever sicherungsbranche. Industriever sicherung und die Zusammenarbeit mit Industriever sicherern ist für Unternehmen in sämtlichen Bereichen des Risikomanagements von essenzieller Bedeutung. Durch unterschiedliche Versicherungskonzernzusammensetzungen und Rechtsformen ergeben sich Schwerpunkte in der Betreuung verschiedener Kundensegmente im Geschäftskundenbereich. Dementsprechend müssen sich die im deutschen Versicherungsmarkt stark untereinander konkurrierenden Versicherer in diesem Bereich unterschiedlichen Kundenanforderungen stellen. Ein ganzheitliches Risikomanagement auf Seiten des Industrieunternehmens sowie auf Seiten des Versicherungsunternehmens ist hierbei, unabhängig von der Art und Größe des Unternehmens, unerlässlich. Nur durch die Identifikation der Risiken, sowie dem Umgang, die Prävention und nicht zuletzt die Absicherung dieser, kann die Wirtschaft wachsen und nach stetigen Innovationen streben. Die sich verändernde Umwelt ist hierbei in Form von Datennutzung sowie Risiko informationsgenerierung und -austausch ein positiver Beschleuniger der Industriever sicherungsbranche, gleichzeitig fordern die Veränderungen neue und innovative

C. Lohmann (✉)

HDI Deutschland, Hannover, Deutschland

E-Mail: christopher.lohmann@hdi.de

S. Sowietzki

AXA XL Deutschland, Köln, Deutschland

E-Mail: stefan.sowietzki@axaxl.com

P. Gewand

TH Köln, Institut für Versicherungswesen, Köln, Deutschland

Risikomanagement- und Versicherungsansätze zur Erhaltung der Sicherheit für die deutsche Industrie.

16.1 Einleitung

Die Versicherung industrieller Risiken ist ein wichtiger Teil des ganzheitlichen Risikomanagements von Unternehmen. Mit dem Abschluss von Versicherungen transferieren Unternehmen Risiken von der eigenen Bilanz auf die Bilanz eines Dritten. Dieser Transfer ermöglicht, dass sich Unternehmen auf die erfolgreiche Bewältigung unternehmerischer Risiken fokussieren können, er glättet Erträge und schafft Planungssicherheit. Damit trägt die Versicherung industrieller Risiken wesentlich zur Entwicklung neuer Geschäftsmodelle und letztlich zu Innovation bei. Aufgrund der Individualität und Komplexität der versicherten industriellen Unternehmen und ihrer Risiken sind auch deren Versicherungen in hohem Maße individuell. Das Angebot an speziellen, individualisierten Produkten und Dienstleistungen ist charakteristisch für das Produkt Industriever sicherung – und die Industriever sicherer in ihrem Anspruch, Unternehmen in allen Phasen ihrer Tätigkeit zur Seite zu stehen.

Die (zunehmende) Relevanz von Industriever sicherung für Unternehmen und in der Folge die Gesamtwirtschaft wird beispielhaft durch einige vom Gesamtverband der Deutschen Versicherungswirtschaft (GDV) veröffentlichte Schadenzahlen der Industriever sicherung deutlich. Obwohl Industriever sicherer das Ziel verfolgen, gemeinsam mit ihren Kunden Schäden zu vermeiden (Prävention), wachsen die von Industriever sicherern für deutsche Risiken getätigten Schadenzahlungen stetig. Wurden im Jahr 2010 Schäden in Höhe von 1,96 Milliarden Euro reguliert, belaufen sich die Schadenzahlungen der deutschen Industriever sicherer in der industriellen Sachversicherung im Jahr 2016 insgesamt auf knapp 2,8 Milliarden Euro (vgl. GDV 2019a). Diese Steigerung spiegelt die zunehmende Durchdringung des Marktes für Industrierisiken, aber auch den Trend zu größeren Schäden einer global immer stärker vernetzten und stark wachsenden Weltwirtschaft wider. Die zwölf höchsten Schäden seit 1962 beinhalten sieben Schäden, die nach dem Jahr 2010 eingetreten sind. Hierunter fällt der aktuell höchste Schaden in Deutschland, der 2016 in der Chemie-Branche eingetreten ist und eine Gesamtschadenhöhe von 464 Millionen Euro aufweist.

Dieses Kapitel gibt einen Überblick über die Branche der Industriever sicherung sowie deren Besonderheiten. Das Kapitel ist in vier Teile untergliedert. Im ersten Teil wird in die Thematik eingeführt. Nach dem Versuch einer Definition und Abgrenzung der Industriever sicherung sowie einem Überblick über Markt und Kunden zu geben, wird auf Spezifika der Organisationsstruktur sowie Rechtsform von Industriever sicherern eingegangen. Dann wird die Rolle von Industriever sicherern im Risikomanagement der Unternehmenskunden thematisiert. Insbesondere wird hierbei auf die Relevanz der Industriever sicherung für die Wirtschaft eingegangen sowie Versicherung als Teil des Risikomanagements im Industrie-

unternehmen herausgearbeitet. Gleichermaßen relevant ist der dritte Teil, die Risikosteuerung der Industriever sicherer selbst. Erläutert werden die Beschaffung von Risiko informationen, die Risikobewertung sowie die wichtige Risikoteilung durch Versicherungs unternehmen, etwa in Konsortialstrukturen oder durch Rückversicherung. Mit aktuellen Veränderungen in der Industrie ändern sich deren Risiken. Die sich hieraus ergebenden zukünftigen Anforderungen für die Industriever sicherer sind immens. Drei dieser Entwicklungen werden im letzten Teil dieses Kapitels dargestellt. Eingegangen wird dabei auf die Megatrends Globalisierung und Digitalisierung sowie die Cyberversicherung als eine moderne Antwort darauf.

16.2 Industriever sicherung und Industriever sicherer

Versicherungsunternehmen differenzieren bei der Entwicklung von Angeboten in der Regel nach zwei Zielgruppen: Privatpersonen und Unternehmen. Während (vereinfacht) die Versicherung von Privatkunden auf den Risikoausgleich in großen Kollektiven sowie Erzielung von Skaleneffekten fokussiert ist, etwa durch standardisierte (wenn auch zunehmend modulare) Produktangebote und automatisierte Verarbeitungsprozesse, ist die Versicherung von insbesondere großen Unternehmen durch individuelle, maßgeschneiderte Risikoabsicherungsprodukte und komplexe Prozessabläufe charakterisiert. Diese Unterscheidung gilt umso stärker, je größer die versicherten Unternehmen sind: Während die Versicherung von kleinen Gewerberisiken zunehmend den Logiken des Marktes für Privatkunden (Retailmarkt) folgt, ist die Versicherung großer industrieller und spezieller Risiken noch heute „Manufaktur“. Die mit der Digitalisierung einhergehenden Möglichkeiten der Automatisierung oder der Nutzung von Daten verschieben diese Grenze laufend. Trotzdem gilt weiter, dass sich mit den Geschäftsmodellen auch die Organisationsstrukturen der Risikoträger von Industrierisiken (Expertenorganisation) von denen des Privatkundensegments (Prozessorganisation) unterscheiden.

16.2.1 Was ist Industrie, was Industriever sicherung?

Bei der Absicherung betrieblicher Risiken von Unternehmen wird in der Regel zwischen Gewerbe- und Industriever sicherung unterschieden. Letztere bezieht sich grundsätzlich auf die Absicherung von größeren, oft global operierenden Industrieunternehmen und deren Risiken. Eine klare, einheitliche Definition von Industrieunternehmen und damit von Industriever sicherung existiert dabei nicht; sie scheint vor dem Hintergrund der Komplexität, Spezifika und Unterschiedlichkeit der Risiken und ihrer Versicherung auch kaum möglich. Damit muss der Gegenstand dessen, was wir in diesem Kapitel analysieren wollen, vage bleiben.

Was verstehen wir hier unter Industriever sicherung?

Erster Ansatzpunkt ist der Blick in die gesetzlichen Grundlagen. Denn jenseits der von Versicherungsunternehmen selbst festgelegten Kriterien werden Großrisiken auch gesetzlich definiert, konkret im § 210 Abs. 2 Nr. 3 VVG. Unternehmen gelten demnach als „Großrisiken“, wenn mindestens zwei der nachstehenden Kriterien erfüllt sind:

- Bilanzsumme größer als 6,2 Millionen Euro;
- Nettoumsatzerlöse größer als 12,8 Millionen Euro;
- Durchschnittliche Arbeitnehmeranzahl von mindestens 250 pro Wirtschaftsjahr.

„Industriever sicherer“ wären nach diesem Verständnis also Risikoträger, die Risiken der so definierten Unternehmensgruppe mit Großrisiken gegen die Zahlung einer Versicherungsprämie übernehmen. Die hier herangezogenen Schwellenwerte scheinen allerdings für ein Verständnis von „Industrie“ bzw. „Industriever sicherung“ niedrig und dürften angesichts moderner technischer Möglichkeiten, Risiken automatisiert zu analysieren und zu versichern, in vielen Häusern eher als Gewerbe-, allenfalls als Firmen-, kaum aber als Industrierisiken verstanden werden.

In der Versicherungsbranche selbst folgt die Aufteilung in Gewerbe bzw. Industrie oft Kriterien, die Versicherer individuell festlegen und anwenden. Zu solchen Kriterien gehört regelmäßig die Unternehmensgröße, die wiederum an Parametern wie Mitarbeiteranzahl und vor allem Jahresumsatz gemessen wird. Da sich Unternehmen gleicher Größe aber in ihren Risikoprofilen signifikant unterscheiden können, sind derlei Kriterien allenfalls als grobe Hilfsgrößen oder Proxi zu verstehen, Risiken nach ihrer Komplexität und den notwendigen Geschäftsmodellen zu differenzieren.

Zielführender scheint, an den Spezifika des zu transferierenden Risikos sowie der nachgefragten Versicherungslösung und -dienstleistung anzusetzen. Dahinter steht die Überlegung, dass aufgrund der für Industrierisiken kennzeichnenden Individualität der Risiken seitens der Industriever sicherer besondere Expertise erforderlich ist. In den Fachbereichen von Industriever sicherern wird daher ein hoher Spezialisierungsgrad benötigt und es sind in der Regel zusätzliche Funktionen wie Underwriting oder Risk Management eingebunden, bevor ein Risikotransfer überhaupt möglich wird. Folglich sind bei Industriever sicherern auch weitaus mehr Berufsbilder als Versicherungskaufleute und Betriebswirte vertreten. So sind Ingenieure unerlässlich bei der Bewertung von industriellen Sachrisiken, Juristen für die Beurteilung haftungsrechtlicher Thematiken der Versicherungsnehmer sowie Mathematiker, Informatiker und Aktuare zum Beispiel in Bezug auf die finanzielle Bewertung der Schadenpotenziale und der entsprechenden Preiskalkulation. Vor dem Hintergrund zunehmender Wetterphänomene oder stofflicher Risiken finden auch Naturwissenschaftler oder Mediziner in der Industriever sicherung ihren Platz.

Ergänzend wird gerne der Grad der Internationalität in der Ausrichtung von Unternehmenskunden als Kriterium zur Differenzierung von Unternehmensversicherungen herangezogen: Global agierende Unternehmen fragen Versicherungsschutz rund um den Globus und daraus folgend die Administration von internationalen Versicherungsprogrammen nach, die neben einer Masterpolice im Heimatland lokale Polices und Deckungskonzepte

in vielen Ländern ganz unterschiedlicher Jurisdiktion erforderlich macht. Internationalität von Versicherungsprogrammen gilt aufgrund der daraus folgenden Komplexität daher oft als kennzeichnend für Industriever sicherung.

Annähern ließe sich eine Definition von „Industriever sicherung“ schließlich über das Risikokollektiv und sein Schadenverhalten. Erstes ist vor dem Hintergrund der eher kleinen Zielgruppe im Industriever sicherungsgeschäft klein, die Schadefrequenz geringer als im Privatkundengeschäft, das Schadenausmaß dafür in der Regel erheblich größer. Industriever sicherer müssen also, anders als Versicherer im Privatkundensegment, finanziell in der Lage sein, potenziell hohe Schadenaufwendungen decken und bilanziell verarbeiten zu können. Demzufolge ist das versicherungstechnische Ergebnis in der Regel volatile. Während im Privatversicherungsbereich der Ausgleich primär im Kollektiv geschaffen wird, spielt in der Industriever sicherung zusätzlich der Ausgleich in der Zeit, etwa über Alternative Risikotransfers, eine zentrale Rolle. Zudem werden Industrierisiken oft nicht nur von einzelnen Versicherungen sondern von Kollektiven (Beteiligung, Rückversicherung) getragen und geteilt. Die Organisation solcher Kollektive oder von Instrumenten alternativen Risikotransfers setzt wiederum spezifische Kompetenzen voraus und kann damit als Abgrenzungskriterium herangezogen werden.

Wie auch immer die Zielgruppe abgegrenzt wird, eines dürfen wir hier vereinfachend annehmen: Die Nachfrager von Industriever sicherungsprodukten gehören der klassischen Fertigungsindustrie ebenso wie Handels- und Dienstleistungsunternehmen an (vgl. Brühwiler 1994, S. 9 f.). In diesem Kapitel verstehen wir diese Unternehmen als „Industrieunternehmen“, da es für die Zwecke dieser Einleitung einer Differenzierung nicht bedarf.

16.2.2 Industriever sicherung in Deutschland: Versicherer

Der Anteil der Industriever sicherer am Gesamtversicherungsmarkt ist, gemessen an Umsatz und Prämie, verhältnismäßig klein. Er kann nur in Ansätzen beziffert werden, da die Abgrenzung der Segmente des Versicherungsgeschäftes mit Unternehmenskunden, wie erläutert, schwer zu bestimmen ist und Industriever sicherer unterschiedliche Grenzen setzen.

Industriever sicherung ist, wie skizziert, ein globales Geschäft, da die zu versichernden Unternehmen in der Regel Risiken in vielen Ländern absichern müssen und hohe Kapazitäten benötigen. Aufgrund der Bedeutung Deutschlands als Industrie- und Dienstleistungsstandort ist die Versicherung von Industrierisiken in Deutschland volumenstark und insofern attraktiv für Versicherer aus aller Welt. Stark vereinfacht lässt sich der Markt unterteilen in global tätige Versicherungsunternehmen, deren Muttergesellschaft in Deutschland sitzt, global tätige ausländische Versicherungsgruppen, die in Deutschland eine Niederlassung oder Tochtergesellschaft unterhalten (oft auch Spezialversicherer) sowie kleinere deutsche Versicherer, die als Teil globaler Netzwerke Versicherungsschutz anbieten.

Zur skizzierten ersten Gruppe gehört die Allianz Global Corporate & Specialty SE (AGCS), der international tätige Industriever sicherer der Allianz Gruppe. Wie die Muttergesellschaft Allianz SE hat die AGCS ihren Sitz in München. Sie agiert selbst weltweit in aktuell 34, durch das Netzwerk der Allianz Gruppe sogar in mehr als 150 Ländern. Auch im (kleineren) deutschen Talanx-Konzern existieren mit der HDI Global SE und der kürzlich gegründeten HDI Global Specialty SE eigene Versicherungsgesellschaften für das Industriegeschäft. Beide Gesellschaften sind mit Niederlassungen, Tochter- und Schwester gesellschaften sowie Netzwerkpartnern in mehr als 150 Ländern weltweit vertreten. Der Hauptsitz von Talanx und HDI Global ist Hannover.

Zur Gruppe der in Deutschland tätigen Industriever sicherer aus aller Welt zählt die AXA XL, eine Tochtergesellschaft des französischen Versicherungskonzerns AXA SA. Sie ist innerhalb des AXA Konzerns für die weltweite Zeichnung von Industrierisiken verantwortlich, auch in Deutschland. Die zugehörige deutsche Gesellschaft der AXA XL Germany ist in den Städten Hamburg, Köln, Frankfurt und München vertreten und Teil des internationalen Netzwerkes von AXA XL und AXA Gruppe. Weitere wichtige (und ähnliche) Beispiele für die Gruppe der ausländischen, in Deutschland operierenden Industriever sicherer sind die Zurich Insurance Company Ltd, eine Tochter der Zurich Gruppe in der Schweiz, die deutschen Tochtergesellschaften und Niederlassungen der American Insurance Group (AIG), von Berkshire Hathaway oder der Chubb (alle mit Muttergesellschaften in den USA), die Mitsui Sumitomo (Japan), sowie die FM Global, ein insbesondere in der industriellen Sachversicherung sehr bedeutender amerikanische VVaG. Auch die Swiss Re Corporate Solutions, ein Teilbereich der weltweit führenden Rückversicherungsgruppe Swiss Re, zeichnet Industrierisiken direkt. Nicht zu vergessen ist der britische Lloyds, eine Repräsentanz der weltberühmten Versicherungsplattform für Industrie und Spezialrisiken in London.

Zur dritten Gruppe der vor allem lokalen Versicherungsunternehmen, die (auch) Industrierisiken versichert, gehören zum Beispiel die Ergo Versicherung, die R+V Allgemeine, die Gothaer Allgemeine Versicherung oder die Württembergische Versicherung. Dieser Gruppe von Versicherungsunternehmen ist gemein, dass sie vorwiegend in Deutschland tätig sind, über Mitgliedschaften in globalen Netzwerken lokaler Versicherer oder durch eigene Kooperationen aber auch Risiken außerhalb Deutschlands und der EU versichern (vgl. GDV 2019).

Schon diese kurze, bei weitem nicht vollständige und durchaus schematische Auflistung verdeutlicht die Breite des Angebots, auf das deutsche Versicherungsnehmer zurückgreifen können. Es ist klar, dass die jeweiligen Anbieter unterschiedliche Strategien verfolgen und unterschiedliche Zielkunden erreichen wollen. Sehr große Industrierisiken etwa, die Versicherungsschutz mit hohen Kapazitäten und in vielen Ländern benötigen, werden Versicherungskonsortien suchen, die in der Regel von den großen, globalen und meist an der Börse notierten Gruppen geführt werden. Kleinere, lokale Versicherer beteiligen sich an solchen Konsortien, führen sie aber nur selten. Mittelständische Kunden wiederum schätzen Versicherungspartner ihren Zuschnitts und ihrer Größe; in der Folge führen die in der dritten Gruppe aufgeführten Versicherer durchaus auch internationale

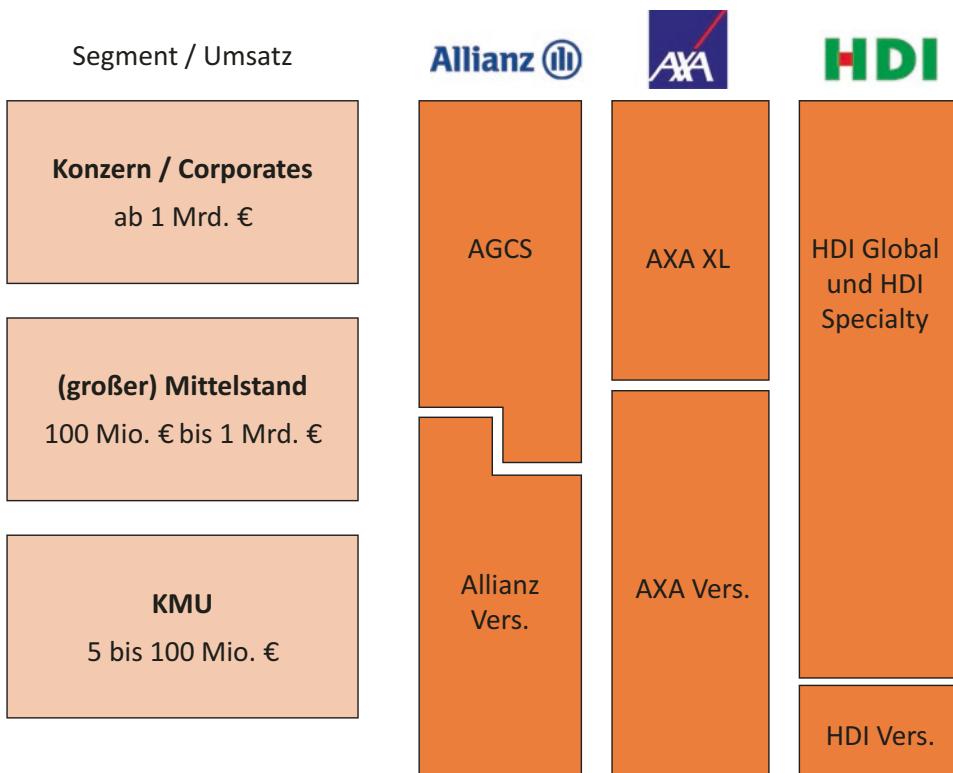


Abb. 16.1 Segmentierung des deutschen Industriever sicherungsmarktes. (Quelle: eigene Darstellung)

Programme, fast ausschließlich aber von mittelständischen Kunden, die von Deutschland aus in begrenztem Maße ins Ausland expandieren.

Wie bereits ausgeführt wurde, kann die Abgrenzung in Gewerbe- und Industiekunden nicht pauschal für die ganze Branche beschrieben oder dargestellt werden, da die verschiedenen Versicherer ganz unterschiedliche Segmentierungen nach ganz unterschiedlichen Kriterien vornehmen. Die nachstehende Darstellung zeigt, wie die großen deutschen Industriever sicherer Marktsegmente konkret definieren und welche Zuständigkeiten der einzelnen Gesellschaften sich entsprechend der Segmentierung ergeben. Abb. 16.1 stellt dar, wie die größten Industriever sicherer in Deutschland ihr Geschäft mit Unternehmerkunden in verschiedenen Konzern-Tochterunternehmen betreuen, um den Anforderungen unterschiedlicher Kunden und Geschäftsmodelle gerecht zu werden – und um ihr Versicherungssortefolio zu steuern.

Während AXA und HDI die Zuständigkeit der verschiedenen Versicherungsgesellschaften im Konzern weitgehend an der Umsatzgröße des Versicherungsnehmers bemessen, spielt im Allianz Konzern die Internationalität des Kunden eine größere Rolle. Grundsätzlich zeichnet AGCS für Unternehmen ab einer Umsatzsumme von 500 Millionen Euro

Geschäft. Sollte der Versicherungsnehmer jedoch über mindestens vier Auslandsstandorte verfügen, die eigener Versicherungslösungen bedürfen, so gilt die Zuständigkeit der AGCS für solche Unternehmen bereits ab einem Umsatz von 250 Millionen Euro. Die Frage der Komplexität der Risiken und damit der konkreten Anforderungen der Zielgruppe spielt hier also eine dezidiertere Rolle als bei den skizzierten reinen Proxi-Modellen.

Die Zurich Versicherung geht noch weiter. Sie berücksichtigt bei der Zuordnung der Segmente und dessen Zuständigkeit vornehmlich die Internationalität des Versicherungsnehmers; Umsatzgrößen werden nicht mehr betrachtet. Internationales Geschäft wird ausschließlich von der Zurich Commercial Insurance gezeichnet und hier wiederum je nach Bedarf an Lokal-Policen in „Large Commercial Geschäft“ und „Mid Market Geschäft“ unterschieden. Das nationale Geschäft fällt in die Zuständigkeit der Zurich Retail Insurance. Ausschlaggebend ist neben der Internationalität der Kunden auch die Komplexität des geforderten Versicherungsschutzes. So erfolgt die Zuordnung in Haftpflicht beispielsweise nach Betriebsarten und Produkten.

Einen anderen Ansatz verfolgt die Gothaer Allgemeine. Sie ordnet ihr Geschäft mit Firmenkunden nach der Komplexität des Risikos in zwei Bereiche. Alle Risiken (Unternehmen), die regelbasiert automatisch gezeichnet werden können, sind Gewerbe. Sie sind Zielgruppe für das Produkt Gothaer GewerbeProtect (GGP), da die Komplexität der Unternehmen und damit ihre Risikobewertung nicht die Underwriting-Fähigkeiten der Informationstechnologie (GoSmart) überschreiten. Risiken hingegen, die aufgrund der Spezifika (noch) nicht automatisiert „underwritten“ werden können, werden durch Underwriter und Risikoingenieure analysiert und entschieden. Expertise, Know-How und auch menschliche Intuition zählen im Segment „Individual“. Es wird erwartet, dass mit zunehmender Leistungsfähigkeit der Informationstechnologie dieses Segment kleiner wird. Interessant ist, dass statt herkömmlicher Größenkriterien spezifischere Bemessungsgrößen für Komplexität des Risikos herangezogen werden, wie etwa hohe Versicherungssummen in den Inhalts-, Gebäude-, Maschinen- und Werksverkehr-Versicherungen. Für die Vermögensschaden-Haftpflichtversicherung erfolgt die Bestimmung nach der Deckungssumme. Lediglich die Betriebs-Haftpflichtversicherung orientiert sich noch am Umsatz der Versicherungsnehmer.

16.2.3 Industriever sicherung in Deutschland: Intermediäre

Versicherungsprodukte sind für Kunden komplex und stellen qua Definition ein in die Zukunft gerichtetes Leistungsversprechen dar; im Moment des Vertragsschlusses ist die Leistung noch nicht greifbar. Daher gilt es für Versicherer, Vertrauensverhältnisse zu seinen Kunden aufzubauen, um die Sicherheit, die das Produkt verspricht, glaubhaft zu kommunizieren.

Durch die Besonderheit des Versicherungsproduktes spielen jedoch auch der Vertrieb und die Betreuung durch unterschiedliche Vermittler eine große Rolle. Grundsätzlich zu unterscheiden sind dabei Vermittler, die (ausschließlich) für einen (einige wenige) Versi-

cherer tätig sind, also „im Lager“ des Versicherers stehen, von unabhängigen Vermittlern, den Maklern. Sie stehen gemäß § 59 Abs. 3 VVG im Lager der Versicherungsnehmer und sind somit Teil des Kundenumfelds, das es für den Industriever sicherer zu beachten und zu managen gilt. Denn in der Regel adressieren Versicherer ihre Industrikunden selten direkt, sondern über die sie betreuenden und beratenden Vermittler.

Für die hier analysierten Industriever sicherer sind unabhängige Makler von mit Abstand größter Bedeutung. Das liegt zum einen daran, dass Unternehmenslenker (Unternehmer wie angestellte Manager) aus „Good Governance“ Erwägungen heraus sicherstellen wollen und müssen, dass sie für „ihr“ Unternehmen den bestmöglichen Versicherungsschutz zu einem attraktiven Preis einkaufen. Risikomanagement und damit auch das Vehikel der Versicherung gehört zu den Pflichten von Unternehmensleitern, einen geordneten Geschäftsbetrieb zu organisieren. Schon aus dieser Organisationspflicht heraus ergibt sich die Notwendigkeit, beim Einkauf von Dienstleistungen wie dem Risikotransfer das beste Angebot auf dem Markt zu identifizieren und anzunehmen. Aus der Unabhängigkeit folgt die Verpflichtung von ebenso unabhängigen Maklern, wollen Unternehmen den Marktvergleich nicht selbst vornehmen. Exklusiv an einen Versicherer gebundene Vermittler sind hierfür keine Alternative. Die Verpflichtung leistungsstarker Vermittler folgt zum anderen aber auch der Komplexität der zu transferierenden Risiken, insbesondere (aber nicht allein) bei global tätigen Unternehmen. Die Versicherungsprogramme sind in der Konstruktion wie im Handling so anspruchsvoll, dass nur hochprofessionelle Vermittler dem Unternehmensleiter ein guter, unabhängiger Berater und Vermittler sein können. Auch diesem Anspruch werden Exklusivvermittler in der Regel nicht gerecht.

Abb. 16.2 des Versicherungsmonitors gibt einen aktuellen Überblick über die größten in Deutschland tätigen Maklerhäuser.

Versicherungsmonitor-Analyse: Die größten Makler 2018				
Provisions- und Honorarumsätze der größten Industriever sicherungsmakler aus deutschem Geschäft in Millionen Euro Unternehmensangaben oder Schätzung des Versicherungsmonitors				
Rang	Firma	Industrie	Gesamt (1)	Quelle
1	Ecclesia	172	217 (2)	Unternehmen
2	Aon	170	250	Schätzung VM
3	Marsh	135	135	Schätzung VM
4	Funk	124	137	Unternehmen
5	Martens & Prahl	102	102	Unternehmen
6	Leue & Nill	55	55	Unternehmen
7	Willis	50	200	Schätzung VM
8	Artus Gruppe	45	48	Unternehmen
9	MRH Trowe (3)	42	42	Unternehmen
10	Südvers	40	40	Unternehmen
11	Schunck	34	34	Unternehmen

(1) Umfasst Industrie sowie andere Aktivitäten (Privatkundengeschäft, Altersvorsorge, Beratung)
(2) Gruppenumsatz mit Ausland
(3) Mit Nofri, zum 1. Januar 2019 übernommen

Abb. 16.2 Versicherungsmonitor-Analyse: Die größten Makler 2018. (Quelle: eigene Darstellung in Anlehnung an Fromme 2019)

Zu unterscheiden sind hier Tochtergesellschaften global tätiger Maklerkonzerne wie AON, Marsh und Willis von in der Regel inhabergeführten mittelständischen Häusern. Letztere sind lange im deutschen Markt tätig und haben über Jahre erfolgreichen Wachstums eine Größe und Expertise erreicht, die sie auf Augenhöhe mit globalen Maklerhäusern operieren lässt. Auch in Bezug auf den passenden Makler hat der Industriekunde in einem gut entwickelten Markt also die „Qual der Wahl“ und wird abwägen zwischen Qualität des internationalen Netzwerkes, Expertise in der Beurteilung und Platzierung von Risiken – und Kundennähe.

Anders als in fast allen anderen Märkten ist in Deutschland die Gruppe der firmenverbundenen Vermittler (FVV) weiter ausgeprägt. Diese im Gesamtverband der versicherungsnehmenden Wirtschaft (GVNW) organisierten Gruppe von Vermittlern gehört dem Industriekunden selbst und ist bis auf Ausnahmen ausschließlich in die Platzierung von Risiken für den Unternehmensverbund eingebunden, zu der sie gehört. Für den Erhalt dieser sehr speziellen Vermittlergruppe können steuerliche sowie Kostengründe maßgeblich sein; durch die enge Einbindung in ein Unternehmen sind FVVS zudem mit den Risiken vertraut und können insbesondere bei Risikomanagement und -reduzierung eine wichtige Transmissionsrolle spielen. Interessanterweise ist diese Form von Vermittlung und Einbindung (Versicherer wickeln über FVVs ihr Geschäft quasi direkt ab) in angelsächsischen Ländern kaum bekannt.

16.2.4 Industrieversicherung in Deutschland: Kunden

Wie beschrieben haben Unternehmen unterschiedliche Bedürfnisse und Anforderungen an ihren Versicherungsschutz. Dieser Anspruch bezieht sich auch auf den Versicherer und den für sie tätigen Intermediär. Die benötigte Absicherung von Haftstrecken ist beispielsweise unterschiedlich hoch, es sind oder es sind nicht Versicherungslösungen über internationale Programme für Auslandsaktivitäten erforderlich.

Folgt man der Segmentierung in Abb. 16.1, dann lassen sich Unternehmen vereinfacht in die folgenden drei Bereiche unterteilen: Kleine und mittlere Unternehmen, Mittelstand und multinationale Konzerne. Anhand dieser Aufteilung können die unterschiedlichen Bedarfe verschiedener großer Unternehmen noch einmal schematisch verdeutlicht werden.

Kleine und mittlere Unternehmen, welche gängig auch als „KMU“ betitelt werden, beschreiben Unternehmen die einen Umsatz zwischen fünf und 50 Millionen Euro im Jahr erwirtschaften. Durch die überschaubare Größe sind die Anforderungen an den Versicherungsschutz in der Regel durch klassische, oft standardisierte Produkte abdeckbar. Bei dem Versicherungsschutz von kleinen und mittleren Unternehmen gelten außergewöhnliche Besonderheiten eher als Ausnahme. Anstelle von stark individualisierten Deckungskonzepten stehen bei der Wahl des Versicherers und auch des Vermittlers oft der lokale Bezug und eine persönliche Betreuung im Vordergrund. Das gilt insbesondere für Unternehmen, für die Unabhängigkeit des Rates von untergeordneter Bedeutung ist. Bei einer besonderen Ausrichtung des Unternehmens können Nischenmakler die Betreuung der

Versicherungen und die Beratung im Risikomanagement von Vorteil für sein (vgl. Banks 2004, S. 57; vgl. Cummins et al. 2006, S. 360 ff.; Zurich Gruppe Deutschland o. J.).

Das Marktsegment des Mittelstands umfasst Unternehmen, welche einen Umsatz von 50 Millionen Euro bis zu einer Milliarde Euro p. a. erwirtschaften. Mit steigender Unternehmensgröße steigt auch die Komplexität der Risiken. In der Regel agieren Unternehmen in solchen Größenordnungen auch international. So steht im mittleren Marktsegment nicht mehr die lokale Nähe im Vordergrund, sondern die Kompetenz die komplexen Risiken richtig abbilden und versichern zu können. Wie schon zuvor dargestellt sind dies nicht nur Kriterien, welche der Versicherer erfüllen muss. Die Betreuung dieser Kunden erfolgt in aller Regel durch Industriever sicherungsmakler, welche die Kunden umfassend über Versicherungsmöglichkeiten beraten, die Versicherungsverträge betreuen und, ebenso wie die Versicherer, den Kunden auch im Risikomanagement unterstützen. Durch die Makler wird die Informationsasymmetrie zwischen dem Versicherungsnehmer und dem Versicherer bestmöglich ausgeglichen (vgl. Banks 2004, S. 57; vgl. Cummins et al. 2006, S. 360 ff.; vgl. Zurich Gruppe Deutschland o. J.).

Die größten Unternehmen am Markt werden in dem letzten Segment, multinationale Konzerne, erfasst. Unternehmen zählen ab einem Umsatz von einer Milliarde Euro in dieses Segment. Die Individualität und Internationalität der Risiken sind hier noch einmal deutlich ausgeprägter als im zuvor beschriebenen Mittelstand. Solche Risiken werden vor allem von weltweit agierenden Versicherungskonzernen gezeichnet. Sie bringen das internationale Netzwerk sowie die Expertise für die speziell zusammengestellten Versicherungslösungen mit. Auch die Makler müssen für Risiken in dieser Größenordnung neben der Expertise eine entsprechende internationale Infrastruktur für die Betreuung mitbringen. Da die Risiken teilweise nicht über den deutschen Markt abgedeckt werden können, sind hier globale Broker erforderlich, welche auch Zugang zu Spezialmärkten wie Lloyds of London haben (vgl. Banks 2004, S. 57; vgl. Cummins et al. 2006, S. 360 ff.; vgl. Zurich Gruppe Deutschland o. J.).

16.2.5 Organisation von Industriever sicherung

Eine adäquate organisatorische Aufhängung und Struktur ist bei Industriever sicherern vor dem Hintergrund Kapital- und regulatorischer Anforderungen sowie der Logiken ihrer Geschäftsmodelle unabdingbar. Wie für einige Beispiele des Industriever sicherungsmarktes beschrieben, besteht oft eine eigene Tochtergesellschaft für die Versicherung von Industrikunden innerhalb des Konzerns. Das ist aber nur eine Antwort auf die Frage, wie die Zeichnung von Industrierisiken zu organisieren und zu strukturieren sei. Die gefundenen Lösungen sind dabei fast so vielfältig wie die Ansätze zur Definition und Kategorisierung der Risiken.

Bis auf wenige Ausnahmen (etwa FM Global) wird die Versicherung von Industrierisiken nicht stand-alone, sondern innerhalb größerer Einheiten und damit eingebettet in im weitesten Sinne Konzernstrukturen betrieben. Das hat manchmal historische Gründe, ist

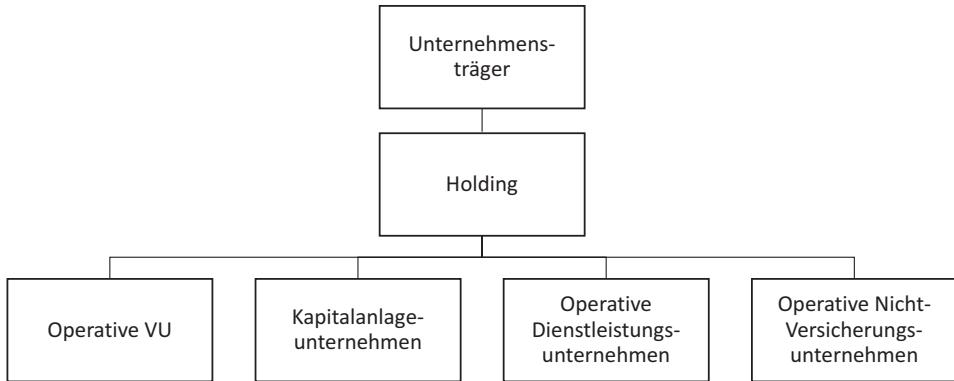


Abb. 16.3 Konzernstruktur von Versicherungsunternehmen. (Quelle: eigene Darstellung in Anlehnung an Farny 2011, S. 257)

aber vor allem in Portfolioüberlegungen (Diversifizierung) oder Möglichkeiten der Skalierung (etwa in der Kapitalanlage) begründet (vgl. Farny 2011, S. 257).

Eine Konzernstruktur erlaubt Versicherungsunternehmen die Zusammenfassung gleicher und die Trennung unterschiedlicher Geschäftsmodelle und Funktionen. Die in Abb. 16.3 dargestellte Konzernstruktur ist dabei häufig vertreten. An der Spitze der Konzernstruktur steht eine Holding, in der Regel eine Aktiengesellschaft oder ein Versicherungsverein auf Gegenseitigkeit, welche die Außenbeziehung, insbesondere zu den Unternehmensträgern, aber auch zur Öffentlichkeit hält. Gleichzeitig ist sie Eigentümer aller Konzerngesellschaften und für die Leitung des Konzerns zuständig. Unter der Holding sind die verschiedenen Unternehmen angesiedelt, welche in der Regel unter operativen Versicherungsunternehmen, Kapitalanlageunternehmen, operativen Dienstleistungsunternehmen oder nicht operativen Nicht-Versicherungsunternehmen subsummiert werden (vgl. Farny 2011, S. 285 f.).

Im Hinblick auf die Einordnung von Industriever sicherern in Versicherungskonzerne ist die Kategorie der operativen Versicherungsunternehmen relevant. Dieser werden Versicherungsunternehmen des Konzerns zugeordnet, die Versicherungsgeschäft zeichnen; dazu gehören auch Industriever sicherer. Diese können als reine Industriever sicherer, wie zum Beispiel die AXA XL, bestehen, oder Teil eines Risikoträgers für diverse private, gewerbliche und industrielle Kundensegmente, wie im Fall der Gothaer Allgemeine Versicherung AG, sein.

Neben der Segmentierung und organisatorischen Zuordnung der Risiken nach Gewerbe und Industrie ist für die Organisationsstruktur von Versicherern auch die Anordnung der Versicherungssparten innerhalb des Segmentes „Industrie“ von Bedeutung. Industriever sicherung wird dabei vereinfacht oft in die Bereiche der Eigenschadenversicherungen, der Drittschadenversicherungen sowie jene Deckungskonzepte gegliedert, die sowohl Eigenschaden- als auch Drittschadenkomponenten aufweisen. Den drei Bereichen sind die gro-

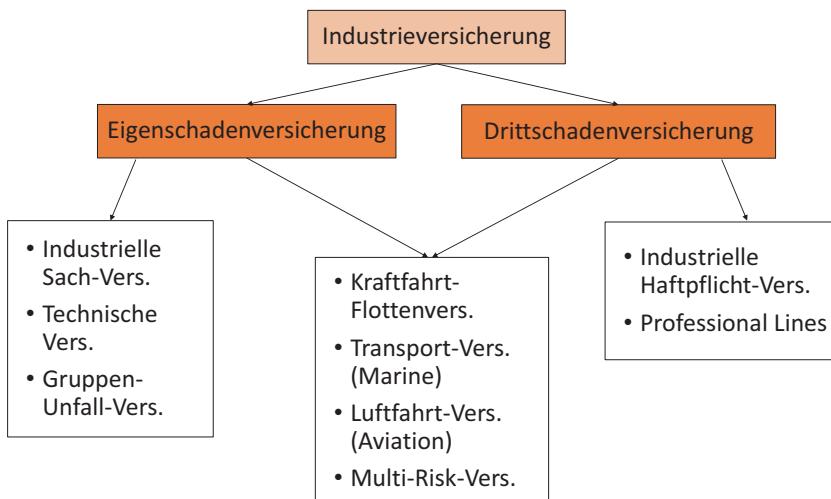


Abb. 16.4 Versicherungszweige/-sparten der Industrie. (Quelle: eigene Darstellung)

ßen Industriever sicherungssparten gemäß Abb. 16.4 zuzuordnen. Ihnen gehören wiederum diverse unterschiedliche einzelne Versicherungslösungen an.

Die Organisationsstruktur des Industriegeschäfts von Versicherern (oft auch noch von Gewerbe) folgt den in Abb. 16.4 dargestellten Versicherungssparten. Dies ist vor allem darauf zurückzuführen, dass die aufsichtsrechtliche Berichterstattung an die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) getrennt nach Sparten erfolgt. Im Ergebnis kann die Geschäftssteuerung des Portfolios auf diese Weise präzise erfolgen, die Expertise in den einzelnen Bereichen ist ausgeprägt und insbesondere im Management der Erträge stehen die versicherungstechnischen Ergebnisse jeder Einzelsparte im Fokus.

Die Spartenstruktur hat aber auch Nachteile. Kunden erwarten, über die einzelnen Sparten hinaus ganzheitlich als ein Kunde (ein Account) betrachtet und betreut zu werden. Die skizzierte Spartentrennung stellt Versicherer dabei vor Herausforderungen. Denn eine Steuerung und Zielvergabe nach Sparten verengt schnell den Blick: Führungskräfte und Underwriter betrachten dann überspitzt ausschließlich Bestand und Verlauf der eigenen Sparte, die ganzheitliche Sicht auf den Kunden geht verloren.

Lösungen können Ertragsbetrachtungen auf Kunden- oder auch auf Maklerebene sein, die explizit die Möglichkeit von Quersubventionierungen vorsehen und die Profitpools einer Sparte (und der Gesamtverbindung) zulasten anderer Sparten schützen. Auch kann eine Betreuung des Kunden am Point of Sale durch Key Accounter oder ein Kundenteam Probleme abfedern. In Ergebnis sind Underwriting-Entscheidungen unter Berücksichtigung des Gesamtkunden komplexer und schwieriger, es gilt ein Gleichgewicht mit der technischen Expertise zu finden. Insgesamt bleibt das Spannungsumfeld, dass Versicherer auf die Versicherungstechnik aller Sparten achten müssen, Kunden und Makler aber den Verlauf ihres Ausschnitts-Portfolios betrachten.

16.2.6 Die Gesellschaftsform des Risikoträgers

Zulässige Gesellschaftsformen für Versicherungsunternehmen sind im § 8 Abs. 2 VAG geregelt. Demnach sind Aktiengesellschaften (AGs) einschließlich der Europäischen Gesellschaft (SE), Versicherungsvereine auf Gegenseitigkeit (VVaGs) sowie Körperschaften und Anstalten des öffentlichen Rechts dazu befugt, in Deutschland Risiken in Form von Versicherungen zu zeichnen.

In der Praxis sind primär die Gesellschaftsformen der Aktiengesellschaft und des Versicherungsvereins auf Gegenseitigkeit in der Versicherung von Industrierisiken vertreten (vgl. Gothaer Konzern 2018, S. 16). Während die AG (SE), auch jenseits der Versicherungswirtschaft, eine übliche Gesellschaftsform in Deutschland (Europa) ist, sind Versicherungsvereine auf Gegenseitigkeit eine spezielle Gesellschaftsform explizit für Versicherungsunternehmen.

Sie zeichnen sich dadurch aus, dass die Versicherungsnehmer Mitglieder des Vereins und somit des Risikoträgers sind. VVaGs enthalten damit Elemente von Wirtschaftsvereinen und Genossenschaften. Eine Vereinsmitgliedschaft erfolgt dabei jedoch nicht durch eine Kapitaleinlage, sondern kann ausschließlich nur durch den Abschluss eines Versicherungsvertrages bei dem entsprechenden VVaG erreicht werden. Somit gilt, dass alle Mitglieder gleichzeitig Versicherungsnehmer, also Kunden, sowie Risikoträger bzw. Eigentümer des Versicherungsvereins, „ihrer“ Versicherung, sind. Die Grundidee dieser Rechtsform baut auf dem Gegenseitigkeitsprinzip und dem Gemeinschaftsgedanken auf (vgl. Farny 2011, S. 205 ff.) und hat in Deutschland große Tradition. VVaGs wie die Alte Leipziger oder Gothaer wurden vor über 200 Jahren gegründet – und existieren im Kern unverändert bis heute.

Da die Kapitaleinlage bei Versicherungsvereinen auf Gegenseitigkeit ausschließlich durch den Abschluss von Versicherungsverträgen erfolgt, haben Versicherungsunternehmen mit dieser Rechtsform, besonders im Vergleich mit Aktiengesellschaften, einen Nachteil bei der Finanzierung. Die Eigenkapitalbildung erfolgt durch Gewinnthesaurierung, die Ausgabe von Genussrechten oder durch Aufnahme nachrangiger Verbindlichkeiten. Ein Zugang zum Markt für echtes Eigenkapital ist nicht möglich (vgl. Farny 2011, S. 205 ff.). Interessanterweise sind Substanz und Finanzstärke von VVaGs im Durchschnitt dennoch besser als bei Kapitalgesellschaften. Dies ist vor allem darauf zurückzuführen, dass bei Aktiengesellschaften Gewinne ausgeschüttet werden, die bei VVaGs mittels Thesaurierung wieder in das Versicherungsunternehmen investiert werden (vgl. Gothaer Konzern 2018, S. 16): Der Zugang zu Eigenkapital hat für AGs einen Preis in Form von Dividenden, die der Kapitalmarkt regelmäßig einfordert. Diese Forderung kennen VVaGs nicht.

Für die Absicherung großer Risiken erweist sich der schnelle Zugang zu Kapital als dominant. Ein Ausgleich schlechter Schadenjahre kann durch verhältnismäßig unkomplizierte Kapitalbeschaffung über das Begeben neuer Aktien erzeugt werden. Die Kapazität, die bei der Absicherung von Konzernen und dem sehr großen Mittelstand zur Verfügung gestellt werden muss, übersteigt oftmals die Möglichkeiten von VVaGs, welche eben keinen Zugang zum Kapitalmarkt finden (Spitzenrisiken können auch durch Rückversiche-

rung oder direkt am Kapitalmarkt in Form von alternativem Risikotransfer abgesichert werden). Diese erwirtschaften die Summe aller erforderlichen liquiden Mittel selber. Die Zielgruppen von VVaGs sind meist, im Bereich der Industriever sicherung, verhältnismäßig kleinere Industrierisiken.

Im Ergebnis sind die weltweit größten Industriever sicherer sowie die Versicherer sehr großer Industrierisiken Aktiengesellschaften. Gründe hierfür sind neben der bereits skizzierten hohen Volatilität der Risiken bzw. des Schadenausmaßes, aber auch die kapitalintensive Notwendigkeit, ein internationales Netzwerk von Versicherungen zu schaffen. Dieses Netz ist bei großen Versicherungsgruppen wie Allianz, AXA, HDI, Zurich, AIG oder Chubb proprietär, bei VVaGs entsteht es in Verbünden.

16.2.7 Märkte und Preise

Das sehr breite Angebot am deutschen Markt für Industriever sicherungsrisiken ist Ausdruck eines gesunden, intensiven Wettbewerbs, der über lange Jahre zu ständigem Preisdruck und stetig sinkenden Preisen führte. Solide Kapitalanlageergebnisse und hohe Verfügbarkeit von Kapital waren wichtige Treiber dieser Spirale „nach unten“. Sie führte dazu, dass in einzelnen Sparten Schadenzahlungen und Kosten regelmäßig die Prämien einnahmen überstiegen.

Mit der Niedrigzinsphase und dem damit einhergehenden Verfall der Kapitalanlageergebnisse änderte sich diese Situation. Ohne substanzelle Erträge aus der Kapitalanlage gewinnt die eigentliche Versicherungstechnik an Bedeutung, Beiträge und Schadenzahlungen müssen wieder im richtigen Verhältnis stehen. Die Märkte reagierten, zunächst durch sich immer weiter konsolidierende Märkte, seit 2018 auch mit dem Einläuten einer Hartmarktphase.

Die angespannte Konkurrenzsituation am Markt, die Suche nach Skalenerträgen, aber auch das Ziel, ein möglichst ganzheitliches Angebot über alle Segmente, Produkte und Regionen präsentieren zu können, führte zuletzt zu einer Konsolidierung des Marktes für Industrierisiken, also zu Übernahmen durch große Versicherungsunternehmen. In jüngerer Vergangenheit sind einige prominente, große Übernahmen im Markt der Industriever sicherer als Konsequenz der Wettbewerbsintensität hervorgegangen. So wurde 2015 Chubb von der ACE übernommen und damit zum größten Sachversicherer weltweit; kurz darauf übernahm die XL Group die Catlin. 2018 wurde die XL Group wiederum von der AXA aufgekauft.

Ebenfalls 2018 hat sich der Zyklus in der Industriever sicherung gedreht, angefangen mit der über viele Jahre defizitären Sachversicherung (Feuer und Betriebsunterbrechung), gefolgt von der D&O Versicherung. Die in diesen Teilmärkten von einzelnen Marktteilnehmern initiierte Verhärtung der Prämie hat bis 2019 auf den gesamten Markt übergegriffen, zuletzt auf die Haftpflichtversicherung. Viele Marktteilnehmer (Kunden, Versicherer, Vermittler) erleben diese Hartmarktphase zum ersten Mal; sie stellt alle vor besondere Herausforderungen. Ihr Ende ist zur Drucklegung dieses Buches offen.

Das Phänomen der Hartmarktphase erklärt sich vor dem Hintergrund der Funktionsweise von Finanzmärkten. Denn wie in den meisten Märkten durchläuft auch der Versicherungsmarkt immer wieder unterschiedliche Marktzyklen, die für eine unbestimmte Zeit anhalten können. Während eines „normalen“ Marktzyklusses befinden sich Angebot und Nachfrage im Gleichgewicht. Durch diesen Ausgleich ergibt sich eine faire Prämie für adäquaten Versicherungsschutz. In der Praxis kommt dieses Szenario sehr selten und wenn dann nur für einen kurzen Zeitraum vor. Sehr viel öfter befindet sich der Industrieverseicherungsmarkt in einem Ungleichgewicht und wir reden von einem harten oder weichen Markt. Diese Marktphasen werden in der Theorie hauptsächlich durch Kapazität und Kapitalerträge beeinflusst. Bei einem hohen Zinsniveau tendieren die Versicherer dazu, die Prämien zu senken und mehr Geschäft zu zeichnen. Die hohen Kapitalerträge helfen, ein mögliches schlechtes versicherungstechnisches Ergebnis ausgleichen zu können. Zu Zeiten von einem niedrigen Zinsniveau erhöhen Versicherer die Prämien und zeichnen im Gegenzug weniger Risiken, da die Versicherer nur limitierte Möglichkeiten haben, Verluste bzw. Schäden durch Kapitalerträge auszugleichen (vgl. Banks 2004, S. 37).

Ein sogenannter weicher Markt äußert sich durch eine große Marktkapazität, die zu geringen, nachgebenden (weichen) Prämien führt. Ein solcher Markt entwickelt sich unter anderem, wenn Versicherer ihr Underwriting offensiv gestalten, um mehr Geschäft zu generieren. Dies ist der Fall, wenn ein Ausgleich eines negativen versicherungstechnischen Ergebnisses durch Kapitalerträge möglich ist oder ein konkurrierendes Marktumfeld, insbesondere in den rentablen Versicherungssparten, besteht (vgl. Banks 2004, S. 37).

Wenn Versicherer ihre Zeichnungskapazität reduzieren und die Prämien teurer (härter) werden, befindet sich der Markt in einer harten Marktphase. Versicherer zeichnen Geschäft zunehmend vorsichtiger und zielen nicht darauf ab „um jeden Preis“ Marktanteile zu generieren (vgl. Banks 2004, S. 37). Die Hintergründe hierfür sind vielschichtig. Eine zurückhaltendere Zeichnungspolitik kann beispielsweise auf unrentables Geschäft in der Vergangenheit zurückzuführen sein. Hierbei muss jedoch berücksichtigt werden, dass sich bei sogenanntem Long-Tail-Geschäft, wie zum Beispiel der Haftpflichtversicherung, viele Schäden erst nach längerer Zeit, in Form von Spätschäden realisieren. Die langfristigen Folgen einer unwirtschaftlichen Zeichnungspolitik werden dementsprechend erst sehr viel später sichtbar – und korrigiert.

Auch wenn sich einige Sparten vor dem Hintergrund der großen Konkurrenz aktuell weiterhin in einer eher weichen Marktphase befinden, waren besonders der Markt der industriellen Sachversicherung sowie der Markt für D&O Versicherungen von großen Schäden und Verlusten seitens der Industrieverseicherer geprägt. Die vergangenen schadenträchtigen Jahre haben zu einer deutlichen Verhärtung des Marktes geführt. Die aktuelle Hartmarktphase ist besonders interessant, weil das Makrophänomen der Verhärtung auf das Mikroverhalten der Spieler zurückgeführt werden kann.

So hat beispielsweise einer der Marktführer der industriellen Sachversicherung, die HDI Global SE, das Projekt 20/20/20 auf den Weg gebracht. Dieses Programm hat das

Ziel, die Preise für 20 Prozent der Sachkunden bis 2020 um 20 Prozent-Punkte zu steigern (vgl. Fromme und Hagen 2019). Preise und Bedingungen sollen angepasst, Anteile bei Bedarf reduziert und untertarifiertes Geschäft aufgegeben werden. Das harte Marktumfeld der industriellen Sachversicherung ist hier deutlich zu erkennen (vgl. HDI Global SE 2019).

Eine ähnliche Verhärtung ist auch im Bereich der Financial Lines zu beobachten. Viele der bestehenden Verträge werden nicht unverändert verlängert. Die Prämien werden angehoben, angebotene Kapazitäten reduziert oder Verträge seitens der Versicherer ganz gekündigt. Auch in anderen Märkten ist die Verhärtung zu spüren, im TV- und Transportgeschäft und auch im noch jungen Geschäftsfeld Cyber (vgl. Fromme und Hagen 2019). Es bleibt abzuwarten wie sich der gesamte Markt weiterentwickelt und wie lange die Hartmarktphase anhält. Ohne Zweifel ist sie eine wichtige Korrektur zur technischen Stärkung der Industriever sicherer.

Diese tut not, denn auch Marktveränderungen wie die Digitalisierung und die Globalisierung von Kunden gehen einher mit einem veränderten Kundenumfeld und hieraus resultierenden Anforderungen. Durch die komplexeren Produkte und Prozesse in der Industrie ergeben sich darüber hinaus neue Risiken. Versicherungsunternehmen antworten darauf mit eigenen Innovationen. In den letzten Jahren entstanden so Produkte der Versicherung gegen Cyber-Risiken, die Betriebsunterbrechung ohne Sachschaden (non-damage business interruption) oder zur Absicherung von parametrischen Risiken. Leistungsfähige, innovative Industriever sicherer aber brauchen angemessene Erträge für ihre Investitionen. Auch dazu leistet die Hartmarktphase einen Beitrag.

16.3 Rolle und Funktion von Industriever sicherung

Unternehmen werden zunehmend internationaler, digitaler und komplexer. Aus den vielschichtigen Unternehmungen gehen immer mehr und größere Risiken hervor, der Investitionsbedarf nimmt zu. Demgegenüber sinkt mit steigendem Risiko die Investitionsbereitschaft von Unternehmen. Unternehmen müssen ständig abwägen, ob sich eine Investition mit Wachstumspotenzial lohnt, ob die Risiken also in einem angemessenen Verhältnis stehen. Der Industriever sicherung kommt bei dieser Abwägung eine wichtige Rolle zu.

16.3.1 Relevanz der Industriever sicherung für die Wirtschaft

Die Versicherungsbranche gehört zu den großen Wirtschaftszweigen der deutschen Finanzbranche und ist für die deutsche Wirtschaft von besonderer Bedeutung. Deutsche Versicherer verwalten einen beachtlichen Anteil des Kapitals und übernehmen eine Kapitalakkumulationsfunktion. Durch die Investition des gesammelten Kapitals kommen die

Versicherungsunternehmen ihrer volkswirtschaftlichen Finanzierungsaufgabe nach. Die Anlage von Prämieneinnahmen und Rückstellungen auf dem Geld- bzw. Kapitalmarkt nimmt großen Einfluss auf dessen Struktur sowie die Kapitalversorgung einzelner Wirtschaftsbereiche. Auch der Bereich der Industriever sicherung hat so einen Anteil am wirtschaftlichen Erfolg Deutschlands (vgl. Eisen und Zweifel 2013, S. 17).

Industriever sicherer nehmen aber noch auf andere Weise Einfluss auf die deutsche Wirtschaft. Mithilfe der Industriever sicherung werden Wirtschaftsprozesse, durch Leistungen im Schadenfall und sowie Betreuung der Risiken, stabilisiert. Sichern sich Unternehmen gegen Risiken und Unw ägbarkeiten ab, stellen sich Chancen und Risiken einer Investition anders (positiver) dar als ohne Versicherung. Kapital, das vor Versicherung für die interne Absicherung von Risiken zurückgestellt wurde, wird freigesetzt und kann für Investitionen genutzt werden. Oft ist Versicherung eine Grundbedingung dafür, dass Unternehmen Risiken überhaupt eingehen, so Chancen nutzen und am Markt bestehen und wachsen können. Dementsprechend bildet Industriever sicherung regelmä ßig eine Grundlage für die Entwicklung neuer Technologien (vgl. BDI 2019; vgl. Eisen und Zweifel 2013, S. 16; vgl. Mikosch 2005, S. 18). Es werden Einzelprojekte abgesichert, die ohne Versicherungsschutz mö glicherweise gar nicht umsetzbar wären. Zusätzlich zur Verfü gung gestellte Services wie Risikomanagement tragen dazu bei, Unternehmen hinsichtlich ihrer Risiken umfassend zu beraten und zu begleiten.

Für kleine und mittlere Unternehmen sorgen Industriever sicherer mit ihren Deckungskonzepten und Versicherungslösungen oft für regelrechten Existenzschutz. Für sie können große Schäden (wie eine abgebrannte Produktionsstätte) mit den daraus folgenden Ertragsausfällen den wirtschaftlichen Ruin bedeuten. Die Existenz großer Industriekonzerne ist aufgrund ihrer Größe sowie ihre breite Aufstellung durch einzelne Schäden selten gefährdet. Durch den Transfer von Risiken erfahren solche Unternehmen jedoch Bilanzschutz. Existenzbedrohend sind für solche Unternehmen Flächenrisiken wie Naturgefahren, die ad hoc mehrere Produktionsstandorte erfassen können oder auch der Ausfall von einzelnen Zulie fernern, die einen großen Wertschöpfungsbeitrag für das Unternehmen leisten. Auch überdurch schnittliche Schadenersatzforderungen Dritter können Unternehmen jeder Größe in ihrer Substanz nachhaltig schwä chen.

Durch Absicherung existenzbedrohenden Schäden erhöht sich die Kreditwürdigkeit der Unternehmen. Insgesamt wird durch Versicherung Schutz von bestehendem Vermögen sichergestellt. Dies führt zu einer besseren Planungssicherheit und bildet ebenso oft die Grundlage dafür, risikobehaftete Geschäfte, mit hohen Ertragsaussichten zu tätigen. Marktgerechter Haftpflichtversicherungsschutz etwa ist ein fortlaufend nachgefragter Be standteil bei Verhandlungen mit Lieferanten, Abnehmern und weiteren Vertragspartnern. Es besteht eine Erhöhung der Wagnisbereitschaft, so eröffnen sich neue Handlungsspiel räume und die Wettbewerbsfähigkeit kann gewährleistet werden (vgl. Eisen und Zweifel 2013, S. 16; vgl. BDI 2019).

16.3.2 Versicherung im Risikomanagement von Industrieunternehmen

Unternehmen sind gesetzlich verpflichtet, Risiken zu überwachen. Durch ein wachsendes Spektrum möglicher Risiken für Unternehmen gewinnt ein adäquates Risikomanagement an Bedeutung.

Hierbei müssen Unternehmen professionell vorgehen und Risiken zunächst systematisch erfassen und anschließend analytisch bewerten. Es gilt die analysierten Risiken richtig zu managen. Risiken können akzeptiert und somit selbst von dem Unternehmen getragen werden. Möglicherweise können Risiken auch durch Prävention verringert oder vermieden werden. Die verbleibenden Risiken werden im Optimalfall gezielt transferiert. Das Vorgehen im Risikomanagement wird für Unternehmen, vor dem Hintergrund der steigenden Komplexität der Risiken sowie der starken Vernetzung dieser, immer aufwendiger und die Unterstützung diesbezüglich seitens der Industriever sicherer und Versicherungsmakler immer wichtiger. Die Versicherer übernehmen hierbei diverse Aufgaben, auch neben dem Risikotransfer. Insgesamt erfahren intelligente Konzepte, internationale Marktkenntnisse und die Bewertung von Versicherungsbedarf zunehmende Relevanz und Berücksichtigung im Risikomanagementprozess, um bestmöglich Risikomanagement und Risikoabsicherung für Unternehmen sicherzustellen (vgl. Willis Tower Watson 2018, S. 4 und 26; vgl. Banks 2004, S. 7 ff.; vgl. Eisen und Zweifel 2013, S. 47 und 109).

16.3.2.1 Risikomanagementprozess

Die internationale Norm ISO 31000 beschäftigt sich mit „Grundlagen des Risikomanagements“ und gilt als Risikostandard für diverse Unternehmen (CGE Risk Management Solutions 2018). In der ISO 31000 werden Leitlinien für die Risikobehandlung von Risiken, denen Organisationen ausgesetzt sind, festgelegt. Ebenso wird der Risikomanagementprozess definiert (vgl. Abb. 16.5; vgl. DIN Deutsches Institut für Normung e. V. 2019).

Der Risikomanagementprozess beginnt damit, dass Unternehmen den Umfang, und die Parameter des Geschäfts bestimmen, welche ein Risikomanagement erfordern. Hierbei wird der Plan für das Vorgehen des Risikomanagements erstellt. Im Nachgang erfolgt dann die Risikoeinschätzung in mehreren Schritten. Ziel des ersten Schrittes, der *Risikoidentifikation*, ist es, eine Liste mit allen Aktivitäten und Prozessen zu erstellen, die Risiken mit sich bringen können. Bei diesen Risiken kann es sich um Personenrisiken oder um Risiken für das Kapital, die Umwelt oder aber die Reputation des Unternehmens handeln. Mittels einer *Risikomatrix* erfolgt eine Einteilung in Risiken mit hohen und geringen Wahrscheinlichkeiten. Die identifizierten relevanten Risiken werden im Anschluss analysiert. Hierbei werden Relationen zwischen der Bedrohung, den Konsequenzen und den zugehörigen Sicherheitsbarrieren hergestellt und aufgezeigt. Es folgt die *Risikoevaluation*, in der die sich ergebenen Risikoszenarien bewertet werden. Diese Bewertung erfolgt in der Regel wieder anhand einer Matrix, die Risiken werden hinsichtlich ihrer Wahrscheinlichkeit und

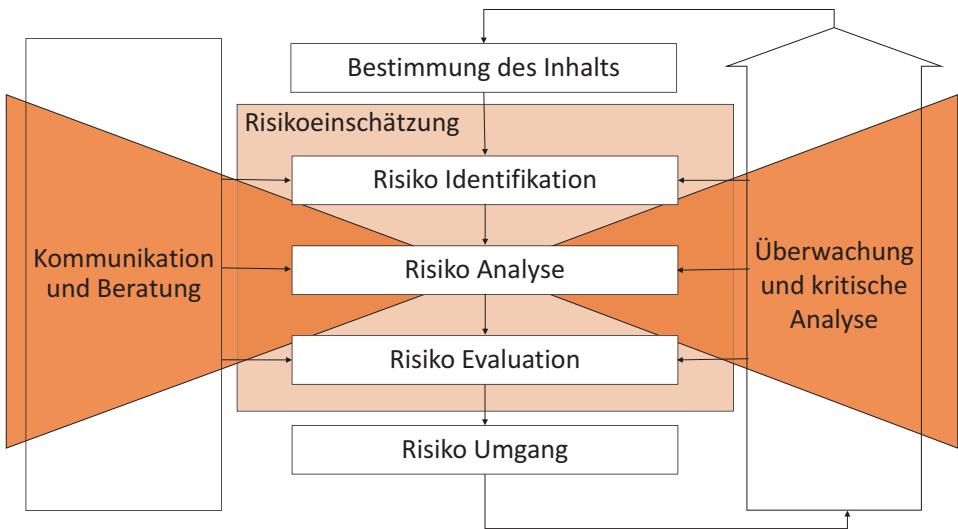


Abb. 16.5 Risikomanagementprozess gemäß ISO 31000. (Quelle: eigene Darstellung in Anlehnung an CGE Risk Management Solutions 2018)

ihres Schweregrades zugeordnet. Damit ist die Risikoeinschätzung abgeschlossen. Die Risikoeinschätzung muss fortlaufend überwacht und kritisch hinterfragt werden. Das Risikomanagement des Unternehmens wird hierbei oft durch externe Beratung unterstützt. Risk Consultants und Versicherer spielen dabei eine bedeutende Rolle (vgl. CGE Risk Management Solutions 2018).

Nachdem die Risiken eingeschätzt worden sind, gilt es, den Umgang zu bestimmen. Risiken können akzeptiert, vermieden bzw. gemindert oder aber transferiert werden.

16.3.2.2 Risikoakzeptanz

Die Akzeptanz von Risiken gehört zur ureigenen Eigenschaft von Unternehmen und Unternehmen. Große Teile des unternehmerischen Risikos sind nicht versicherbar. Doch auch bei versicherbaren Risiken treffen einige Unternehmen die Entscheidung, das Risiko zu akzeptieren und selbst zu tragen. Hierfür gibt es unterschiedliche Gründe. Bei einem umfänglichen Risikomanagement kann aber davon ausgegangen werden, dass solche Entscheidungen bewusst getroffen werden. Die Risiken bzw. Gefahrensituationen werden für die Unternehmen, nach umfänglichen sachlichen Prüfungen und einer Gesamtabwägung, als zumutbar, annehmbar und vertretbar eingestuft und somit für akzeptabel befunden (vgl. Brühwiler 1994, S. 70).

Auch wenn Unternehmen sich bewusst dazu entscheiden, gewisse Risiken zu akzeptieren und selber zu tragen, ist es nicht unüblich, dass Industrieversicherer an dem Prozess beteiligt und in den Risikomanagementprozess involviert sind. Durch selbstgetragene Risiken können, ebenso wie bei transferierten Risiken, Schäden für das jeweilige Unternehmen entstehen. In einem versicherten Schadenfall wird die Schadenabwicklung von dem

Versicherungsunternehmen übernommen. Diese Möglichkeit besteht auch bei nicht versicherten Schäden; Industriever sicherer unterstützen die Schadenbearbeitung zum Beispiel im Eigenbehalt von Unternehmen mit ihrer Expertise durch Servicedienstleistung und Beratung.

Eine weitere besondere Möglichkeit Risiken selbst zu tragen, stellt eine besondere Form der Selbstversicherung dar: Captives. Diese spielen im Management von Selbstbehalten und der Selbstversicherung eine zentrale Rolle. Meist werden sie eingesetzt, um gut kalkulierbare Risiken innerhalb einer Unternehmensgruppe kosteneffektiv zu managen (vgl. Banks 2004, S. 89).

Eine Captive ist ein Versicherungsunternehmen, das von einem nicht in der Versicherungswirtschaft tätigen Unternehmen gegründet wird. Diese Versicherungsgesellschaft übernimmt die Risiken des Unternehmens, bei Gründung durch einen Konzern, die Risiken des Konzerns. Es existieren zwei Ausprägungen von Captives: Erstversicherungs- und Rückversicherung-Captives. Erstere tragen die Risiken des Unternehmens oder des Konzerns direkt, letztere übernehmen die Risiken mittels Fronting über einen zugelassenen Erstversicherer am Markt. Dieser Erstversicherer trägt hierbei kein versicherungstechnisches Risiko, sondern reicht dieses direkt an die Captive weiter, die dann wiederum bei Bedarf Rückversicherungsschutz einkaufen und das Risiko so teilen kann. In der Regel übernehmen Captives nur Risiken eigener Unternehmen, in diesem Fall spricht man von Pure Captives. Eine Broad Captive öffnet sich hingegen dem Markt und versichert auch Risiken fremder bzw. dem Konzern nicht zugehöriger Unternehmen (vgl. Brühwiler 1994, S. 102).

Captives dienen damit letztlich als alternative Art der Risikofinanzierung. Die primären Ziele von Captives sind die Gewinnung von zusätzlichem Kapital, insbesondere auch für neuartige Risiken, der Zugang zum Versicherungsmarkt sowie die Optimierung des Kapitalmanagements im Unternehmen. Letztere wird durch Preisvorteile bei der Selbstversicherung hervorgerufen, während zusätzlich auch die Dividenden der Captive zu einer Steigerung des Cash-Flows führen.

Captives gestalten ihre Geschäftsaktivität analog klassischer Versicherungs- und Rückversicherungsunternehmen, zum Beispiel durch die Bildung von Reserven, durch Risikodiversifikation und durch Risikoteilung über den Rückversicherungsmarkt. Industriever sicherer unterstützen Captives hierbei. Eine Zusammenarbeit ist beispielsweise bei der Preisfindung für bzw. Kalkulation von Risiken üblich, ebenso wie bei der aktuariellen Betrachtung von Schadenszenarien und der Reservekalkulation. Außerdem übernehmen Versicherer Aufgaben im Risikomanagement, welche auch im Fall einer klassischen Versicherung durch den Versicherer ausgeführt werden würden. Hierzu gehört beispielsweise die Ermittlung von Sachrisiken.

Um firmeneigene Versicherung erfolgreich einsetzen und von Vorteilen wie der erweiterten Flexibilität und Wirksamkeit des Risikomanagements profitieren zu können, ist eine gewisse Betriebsgröße vorauszusetzen. Insbesondere vor dem Hintergrund des erforderlichen Kapitals und Aufwand, werden Captives daher nur von sehr großen Industriever sicherungsnehmern gegründet bzw. nachgefragt (vgl. Brühwiler 1994, S. 102 f.).

16.3.2.3 Risikoprävention und Risikovermeidung

Ein Großteil der Risiken von Unternehmen lässt sich mittels Risikoprävention verringern, teilweise sogar komplett vermeiden. Schadenverhütungsmaßnahmen dienen zur Risikoprävention und haben positive Auswirkungen auf die Versicherbarkeit der Risiken und die Versicherungsprämie, aber auch auf finanzielle und strategische Unternehmensziele (vgl. Mikosch 2005, S. 57).

Unter Schadenverhütungsmaßnahmen fallen sämtliche Maßnahmen, durch die die Wahrscheinlichkeit des Schadeneintritts gemindert oder das Schadenausmaß gesenkt wird. Man unterscheidet in technische und organisatorische Schadenverhütungsmaßnahmen. Technische Schadenverhütungsmaßnahmen umfassen technische Anlagen, wie Sprinkler- oder Alarmanlagen, aber auch Vorgehendweisen wie Produktdokumentations- und Ausgangskontrollen sowie bauliche und räumliche Trennungen. Organisatorisch sind hingegen Maßnahmen, die Prozesse und das Verhalten im Schadenfall durch zum Beispiel Notfall- oder Rückrufpläne vorschreiben. Auch vorbeugende Maßnahmen gehören hierzu, so beispielsweise Fahrsicherheitstrainings oder Produktbeobachtungen (vgl. Mikosch 2005, S. 57).

Risikoprävention ist meist Voraussetzung von Industriever sicherern für die Darstellung von Versicherungsschutz. So sind beispielsweise Brandschutzvorkehrungen in der industriellen Sachversicherung notwendig. Vor diesem Hintergrund sind Industriever sicherer in Schadenverhütungsmaßnahmen sehr präsent. Die Versicherungsunternehmen bieten selbst Servicedienstleistungen an und beschäftigen Risk Consultants, die Unternehmen mittels ihrer Beratungskompetenz zur Seite stehen und gleichzeitig die Voraussetzungen für den Versicherungsschutz durchsetzen.

Servicedienstleitungen im Bereich Risikomanagement sind Bestandteil des Angebotes aller Industriever sicherer – genau wie die Übernahme von Risiken. Die AXA XL führt beispielsweise Online bei dem Angebot der Produkte und Dienstleistungen neben Versicherungslösungen das Risk Engineering auf. Mittels spezieller Tablets ist eine schnelle und effiziente Analyse der individuellen Risiken durch die weltweit agierenden Risiko Ingenieure problemlos darstellbar (vgl. AXA 2018).

Die Expertise der Industriever sicherer im Bereich Risikoprävention schafft für Unternehmen nicht nur durch Nachlässe in den Versicherungsprämi en einen Mehrwert. In Falle eines Schadeneintritts gehen selbst bei optimalem Versicherungsschutz Begleiterscheinung aus dem Schaden hervor, welche durch Versicherung nicht abzudecken sind. Hierzu gehören zum Beispiel verlorene Marktanteile, welche durch eine Betriebsunterbrechung des versicherten Unternehmens von Konkurrenten übernommen worden sind. Es lässt sich festhalten, dass die Unterstützung bei der Risikoprävention und der Risikovermeidung durch die Versicherer in der Breite einen großen Mehrwert für die Unternehmen darstellt (vgl. Mikosch 2005, S. 57).

16.3.2.4 Risikotransfer

Versicherung ist eines der bedeutendsten Instrumente für das Risikomanagement von Unternehmen. Der Transfer und die Absicherung von Risiken erfolgen generell durch Versi-

cherung und Derivate. Mittels des Transfers von unsystematischen Risiken können Unternehmen finanzielle Stabilität sicherstellen. Der Transfer von Risiken wird als Verlustfinanzierungstechnik bezeichnet, bei der eine Partei ein Risiko an eine andere Partei verlagert. Hierfür zahlt die risikoverlagernde Partei einen bestimmten Betrag, wie zum Beispiel eine Versicherungsprämie, für die Übernahme des unbestimmten Risikos, an die andere Vertragspartei (vgl. Banks 2004, S. 33 f. und 216).

Durch den Transfer von Risiken werden diese für den Versicherungsnehmer reduziert und quantifizierbar. Die Kosten können kalkuliert werden und für mögliche Schäden müssen keine Rückstellungen in unzumutbarer Höhe gebildet werden.

Für Unternehmen gilt es abzuwagen, welche Risiken transferiert werden sollen und in welchem Umfang der Versicherungsschutz zu gestalten ist. Hierbei müssen die verschiedenen Sparten berücksichtigt werden, ebenso wie die unterschiedlichen möglichen Deckungsbausteine. Zu berücksichtigen sind des Weiteren unterschiedliche Deckungs- bzw. Versicherungssummen, Maximierungen und Selbst behalte. Die Eintrittswahrscheinlichkeit sowie das Ausmaß des Extremereignisses müssen mit der Prämie ins Verhältnis gesetzt werden (vgl. Banks 2004, S. 33 f.).

16.4 Risikosteuerung von Industriever sicherern

Das Geschäftsmodell von Versicherungsunternehmen ist die Übernahme und das Management von Risiken. Ein bedeutender Bestandteil der Geschäftssteuerung ist auch auf Seiten der Versicherer die Abwägung von Chancen und Risiken, die ebenso wichtig ist wie ein entwickeltes Risikobewusstsein. Hierzu gehören eine ausgeprägte Risikomanagementkultur und die Berechnung von Risikokapital genauso wie die Einbindung dieser in wichtige Entscheidungs- und Managementprozesse. Insgesamt gilt für Versicherungsunternehmen, ebenso wie für andere Unternehmen, dass Risiken angemessen identifiziert, analysiert und bewertet werden müssen (vgl. AGCS Hrsg. 2018, S. 16 f.). Darum geht es in diesem Abschnitt.

Die Relevanz eines adäquaten Risikomanagements folgt aus den dafür relevanten gesetzlichen Vorschriften. Gemäß § 89 VAG müssen Versicherungsunternehmen eine aufsichtsrechtlich definierte Risikoreserve zur Sicherstellung der dauernden Erfüllbarkeit ihrer Verträge halten. So soll gewährleistet werden, dass auch im Fall von verlustreichem Versicherungsgeschäft das Versicherungsunternehmen ihren Leistungsversprechen vollständig nachkommen. Die Solvabilitätsvorschriften für die Eigenmittelausstattung von Versicherungsunternehmen sind im EU-einheitlichen System Solvency II geregelt. Ein adäquates Risikomanagement von Versicherern wird durch Vorschriften zur Solvenzkapitalanforderung, zum aufsichtsrechtlichen Überprüfungsprozess sowie zu Publizitätsanforderungen sichergestellt (vgl. Heep-Altiner et al. 2018, S. 1 ff.).

Eine große Rolle spielt in Versicherungsunternehmen die Steuerung des versicherungstechnischen Risikos, das sich primär aus Prämien- und Reserverisiko zusammensetzt. Das Prämienrisiko beschreibt jenes Risiko, bei dem zukünftige Schadenzahlungen nicht von

den eingenommenen Prämien gedeckt werden können. Dieses Risiko wird vor allem durch Zeichnungsrichtlinien gesteuert, die durch Risikoselektion sowie Risikoübernahmevereinschränkungen wie Haftungs- und Versicherungssummen realisiert werden. Die Weitergabe von Risiken mittels Rückversicherung ist ebenfalls ein entscheidender Bestandteil zur Reduzierung des Prämienrisikos von Versicherern. Das Reserverisiko bezieht sich hingegen auf bereits eingetretenen Schäden und deren Abwicklung. Es beschreibt ein Szenario, bei dem Schadenzahlungen aus bereits eingetretenen Schäden die hierfür gebildeten Rückstellungen überschreiten (vgl. AGCS 2018, S. 18).

Da die Individualität und Komplexität der Risiken in der Industriever sicherung enorm hoch sind, sind die Anforderungen der Risikoprüfung und Bewertung von möglichen zu übernehmenden Risiken für die Industriever sicherer ebenfalls sehr umfangreich. Die nicht mögliche Standardisierung vieler Merkmale wird bei der Beschaffung von Risikoinformationen deutlich, ebenso bei der Risikobewertung und möglicher Risikoteilung durch Mit- oder Rückversicherung.

16.4.1 Beschaffung von Risikoinformationen

Risikoinformationen sind ein elementares Instrument der Risikozeichnungspolitik bei der Versicherung von Unternehmensrisiken. Um Risiken zeichnen und vor allem auch, um die Prämien bestimmen zu können, benötigen Versicherer Risikoinformationen (vgl. Cummins et al. 2006, S. 386). Schon durch die Branchenzugehörigkeit lässt sich auf Art, Qualität und Grad des Risikos schließen. Plakativ ist dies für die industriellen Sachversicherung, bei der zum Beispiel die Brennbarkeit der Produkte entscheidend ist, wie auch die Substanz oder der Risikoschutz der Gebäude (vgl. Eisen und Zweifel 2013, S. 197).

Die Risikoinformationsbeschaffung bedeutet Kosten. Durch die hohe Komplexität der Industrierisiken ist die Beschaffung von Risikoinformationen in der Industriever sicherung umfangreicher als in der Privat- oder Kleinkundenversicherung. Nicht selten werden dort spezialisierte Ingenieure eingesetzt, um Risiken, beispielsweise anhand einer Analyse von Produktionsprozessen, zu identifizieren und zu bewerten. Die Ausprägungen der Industrierisiken sind zu komplex, als dass die zugehörigen Prozesse standardisiert werden können. Kosten und Nutzen der Information müssen von Industriever sicherern abgewogen werden (vgl. Eisen und Zweifel 2013, S. 198). Hilfreich sind bei der Beschaffung von Risikoinformationen die gesetzlich vorgeschriebenen vor- und vertraglichen Anzeigepflichten, welchen die Versicherungsnehmer nachkommen müssen (vgl. Mikosch 2005, S. 29).

Versicherer generieren viele der benötigten klassischen Risikoinformationen über Risikofragebögen. Diese werden in regelmäßigen Abständen an die Versicherungsnehmer geschickt, um Aktualität der Informationen sicherzustellen. Die Fragebögen sind in der Industriever sicherung in der Regel sehr viel detaillierter und umfangreicher als in anderen Teilen der Sachversicherung; dies röhrt wieder aus der Komplexität der Risiken, aber auch der in Frage stehenden Versicherungssummen. Oft werden solche Fragebögen für be-

stimmte Risiken individualisiert. Generell erfolgt ein regelmäßiger Austausch über die Risikosituation zwischen dem Versicherungsnehmer und dem Versicherer.

Da die Fragen und deren umfängliche Beantwortung das Risiko nicht komplett abbilden können führen Industriever sicherer auch Risikobesichtigungen vor Ort durch. Große industrielle Sachrisiken werden nicht ohne eine Brandschutzbesichtigung gezeichnet. Auch in der industriellen Haftpflichtversicherung sind Besichtigungen von Produktionsstandorten nicht unüblich. Der durch neue Technologien mögliche Einsatz von Drohnen oder Robotern sowie künstliche Intelligenz zur Auswertung der Aufnahmen ist hierbei hilfreich. Gleichermaßen wird auch zur Auswertung von Schadensfällen verwendet. Generell bieten moderne Technologien auch im Bereich der Risikobewertung einen großen Mehrwert. So können unter anderem Risikodaten aus dem Datenaustausch zwischen Kunden und anderen Partnern des Kunden, wie zum Beispiel Unternehmensberater, einfach und unkompliziert generiert werden.

In vielen Fällen spielt auch der (Industrie-)Makler bei der Informationsbeschaffung eine bedeutende Rolle. Die Zusammenarbeit zwischen Maklern und Versicherungsnehmern besteht oft über einen längeren Zeitraum, weswegen der Makler über viele Risikoinformationen verfügt und den Kunden gut einschätzen kann. Im Falle eines Wechsels des Versicherers helfen die Risikoinformationen sowie die Schadenhistorie dem Versicherer bei der Bewertung der Risiken und dem Makler bei der Platzierung des Risikos (vgl. Cummins et al. 2006, S. 386).

Risikoinformationen sind für einen funktionierenden Versicherungsmarkt unerlässlich. Auch wenn der Markt nicht vollkommen ist, gilt es so viele Risikoinformationen wie möglich in die Bewertung des Risikos einfließen zu lassen (vgl. Cummins et al. 2006, S. 386).

16.4.2 Risikobewertung

Die Bewertung von Industrierisiken erfolgt auf Grundlage der beschafften Risikoinformationen. Sie ist essenziell für das Risikomanagement von Versicherern. Anhand der Bewertung erfolgt nicht nur die risikotechnische Einschätzung des Risikos (Schadeneintrittswahrscheinlichkeit und Schadenausmaß), auf dessen Grundlage eine Risikoprämie bestimmt wird. Durch die Bewertung der einzelnen Risiken ist auch eine Risikoselektion möglich. Entscheidend sind hierbei neben der Risikodiversifizierung auch die zur Verfügung stehende Kapazität sowie die Berücksichtigung von Kumulereignissen, also Schadenereignissen, die auf mehrere versicherte Risiken wirken. Insgesamt ist die Risikobewertung für die Steuerung des versicherungstechnischen Ergebnisses von großer Bedeutung.

Wie in vorherigen Abschnitten ist die Komplexität der Industrierisiken auch in Bezug auf die Risikobewertung wieder besonders herauszustellen. Sie macht die detaillierte Prüfung der Risikoinformationen und eine anschließende individuelle Bewertung

erforderlich. Entsprechende Underwriting-Expertise stellen Industriever sicherer in Fachabteilungen der jeweiligen Versicherungssparten dar.

In der Theorie ergibt sich der Preis für Versicherungsschutz aus der Höhe der erwarteten Schäden des Kollektivs, aus den zugehörigen administrativen und operativen Kosten und einer Rendite für zur Verfügung gestelltes Risikokapital. Bei individuellen und homogenen Risiken ist die Bestimmung der Prämie für den Versicherer unkompliziert. Risiken mit den gleichen Charakteristiken können gruppiert werden, in dem Fall wird für alle Versicherungsverträge die gleiche Prämie erhoben. Heterogene Risiken, welche nicht so einfach klassifiziert werden können, erfordern eine komplexere Bepreisung durch die Industriever sicherer. Anders als in der Privatversicherung ist dies für Industriever sicherer kein Einzelfall. Die Preisfindung erfolgt nach objektiven Ansätzen, durch am Risiko orientierten Rabatten und Zuschlägen ergibt sich jedoch ein subjektiver Spielraum für Underwriter bei der Bestimmung von Prämien. Insgesamt ist die Wahrscheinlichkeit sehr gering, dass die festgesetzten Prämien am Ende genau den entstandenen Kosten entsprechen. Dies wird durch die Komplexität und Individualität der Risiken abermals verstärkt. Zusätzlich zum Ausgleich im Kollektiv erfolgt dann noch der Risikoausgleich in der Zeit, positive Jahre gleichen kostenintensivere Versicherungsperioden aus (vgl. Banks 2004, S. 35 ff.).

Bei der Bewertung von Risiken spielen auch Kumulgefahren eine große Rolle. Diese umfassen das Risiko, dass sich mehrere versicherungstechnische Einheiten, zufällig als nicht unabhängig voneinander herausstellen und so durch ein Ereignis viele Risiken ausgelöst werden. Hieraus ergibt sich, dass angefragte Risiken nicht nur individuell betrachtet werden müssen, sondern auch im Zusammenhang mit Risiken, die sich bereits im Bestand des Versicherers befinden geprüft und analysiert werden müssen (vgl. Farny 2011, S. 85). Hier können Aufschläge erforderlich sein, um dem Risiko und der möglichen erweiterten Absicherung durch Rückversicherung Rechnung zu tragen.

Gleiches gilt auch in Hinblick auf die einem Versicherer zur Verfügung stehende Zeichnungskapazität. Diese stellt das Leistungsvermögen des Versicherungsunternehmens dar, welches für die Übernahme von Risiken besteht. Neben dem Gesamtbestand der Risiken besteht auch auf einzelne Risiken oder Risiken einer Art eine bestimmte Zeichnungskapazität. Diese ergibt sich in erster Linie aus dem verfügbaren Sicherheitskapital des Unternehmens und aus Möglichkeiten von Rückversicherung.

Das zur Verfügung stehende Sicherheitskapital steht auch in Verbindung mit der Rechtsform des Versicherungsunternehmens und dem hieraus resultierenden Zugang zum Eigenkapital.

Essenziell ist bei der Berücksichtigung der Zeichnungskapazität aber ebenso die benötigte Streuung der Risiken im Kollektiv. So müssen Versicherungsunternehmen bei der Bewertung von Risiken auch immer prüfen, ob vor dem Hintergrund der vorgenannten Punkte Zeichnungskapazitäten für die Übernahme des jeweiligen Risikos vorhanden sind (vgl. Farny 2011, S. 631).

16.4.3 Risikoteilung/Risikotransfer

Besonders mit Blick auf den bei der Risikobewertung zu berücksichtigenden Aspekt der Kapazität sind einige Risiken von einzelnen Versicherungsunternehmen nicht allein tragbar. Für den Fall, dass die Versicherungssumme oder Deckungssumme eines zu versichernden Unternehmens die Zeichnungsmöglichkeiten eines einzelnen Versicherers überschreiten, besteht die Möglichkeit der Risikoteilung. Diese kann erfolgen, indem nur ein bestimmter Anteil des versicherten Interesses übernommen wird und die übrigen Anteile von anderen Versicherungsunternehmen getragen werden. In solch einem Fall spricht man von einer offenen Mitversicherung. Eine andere, ebenfalls sehr gängige Methode, nicht das gesamte versicherte Risiko zu tragen, ist der Einkauf von Rückversicherungsschutz. Anders als bei der offenen Mitversicherung, trägt der Erstversicherer gegenüber dem Kunden jedoch das gesamte Risiko. Dieses Risiko transferiert der Versicherer aber wiederum zu Teilen an einen Rückversicherer und übernimmt auf die Art und Weise nur einen Anteil des tatsächlichen Risikos.

16.4.3.1 Offene Mitversicherung

Die offene Mitversicherung umfasst eine anteilige Beteiligung von unterschiedlichen Versicherern an der Versicherung eines versicherten Interesses. Alle Beteiligungen gelten hierbei für denselben Zeitraum und dieselbe versicherte Gefahr (vgl. Schaloske 2013, S. 301).

Die offene Mitversicherung findet insbesondere bei der Versicherung sehr großer oder neuer Risiken Anwendung. Die für solche Risiken erforderliche Kapazität ist für Versicherer oft durch die aufsichtsrechtliche Risikotragfähigkeit oder die festgelegte Zeichnungs politik des Unternehmens nicht allein darstellbar. Vermehrt tritt diese Form der Risikoteilung demzufolge in der industriellen Versicherung auf. Betroffene Sparten sind insbesondere die industrielle Sachversicherung, ebenso wie die industrielle Haftpflichtversicherung, die Technische Versicherung, die Transportversicherung und die Versicherung der sogenannten Professional Risks, die Directors and Officers- sowie die Vermögensschaden-Haftpflichtversicherung inkl. der Cyber-Versicherung. Durch die Risikoteilung des Gesamtrisikos zwischen unterschiedlichen Versicherern erfolgt ein Risiko ausgleich des versicherungstechnischen Gesamtrisikos (vgl. Schaloske 2013, S. 40).

Die Gruppe der an einem versicherten Interesse (mittels offener Mitversicherung) beteiligten Versicherer wird als Konsortium bezeichnet. Dieses wird in aller Regel durch den Makler des Versicherungsnehmers zusammengestellt. Die Versicherer erstellen Angebote für bestimmte Prozentanteile des Risikos, diese werden verglichen und so kombiniert und ggf. angepasst, dass insgesamt 100 Prozent des versicherten Interesses durch das gebildete Konsortium gedeckt sind.

Aus dem Konsortium wird ein führender Versicherer bestimmt. Die Aufgaben sowie eine optionale Vergütung durch eine Führungsprovision von den anderen beteiligten Versicherern werden im Versicherungsvertrag in einer Führungsklausel festgehalten. Der führende Versicherer übernimmt im Regelfall sämtliche Aufgaben, wie die Policierung und

Risikobesichtigungen, die auch im Falle einer Alleinzeichnung vom Versicherer durchgeführt werden, während die anderen beteiligten Versicherer als Kapazitätsgeber fungieren. Im Schadenfall ist es dann auch die Aufgabe des führenden Versicherers den Schaden mit dem Kunden abzuwickeln und entsprechend mit die Regulierungszahlungen der anderen einzufordern.

Eine weitere Alternative der für den Versicherungsnehmer erkennbaren Risikoteilung ist die Exzedenten-Versicherung. Diese findet vermehrt in den Haftpflichtpartien Anwendung. Die Aufteilung der Deckungssumme erfolgt nicht, wie bei der offenen Mitversicherung, prozentual, sondern in verschiedene Deckungsstrecken mit jeweils separaten Verträgen. Wenn die Deckungsstrecke des ersten Vertrages durch Schadenzahlungen aufgebraucht ist, besteht über den hieran anknüpfenden Vertrag eines anderen Versicherers Deckungsschutz. Für Versicherungsunternehmen, die an andere Verträge anschließende Layer zeichnen, stellen die vorangehenden Verträge eine Art Selbstbeteiligung dar. Es ist dabei nicht unüblich, dass Exzedenten-Versicherungsverträge in „following form“ geschlossen werden, sodass die Bedingungen des ersten Vertrages für den oder die folgenden Verträge übernommen werden.

16.4.3.2 Rückversicherung

Rückversicherung ist ein gängiges Risikomanagementtool für Versicherungsunternehmen. Mittels Rückversicherung ist es den Versicherern möglich ihre Brutto-Zeichnungskapazität zu erhöhen. Im Kontext von Erst- und Rückversicherung gilt brutto als Zustand vor der Weitergabe der Risiken an einen Rückversicherer, „netto“ bezeichnet den Zustand nach Rückversicherung. Durch das Schützen von Kapital und gebildeten Reserven wird sichergestellt, dass die Versicherer immer zahlungsfähig sind, ein sogenanntes „Capital Event“ wird verhindert. Des Weiteren können Versicherer ihre Ergebnisse stabilisieren. Der benötigte Risikoausgleich in der Zeit, welcher insbesondere für Industriever sicherer von großer Bedeutung ist, kann durch den Einkauf von Rückversicherung unterstützt werden. Darüber hinaus ist der Schutz der Solvabilität des Erstversicherers sowie das hiermit verbundene bessere Rating ein weiterer Grund für den Einkauf von Rückversicherung (vgl. Banks 2004, S. 53; vgl. Eisen und Zweifel 2013, S. 207).

Man unterscheidet fakultative und obligatorische Rückversicherung. Während bei der obligatorischen Rückversicherung ein gesamtes Portfolio rückversichert wird und demzufolge jedes in dem Portfolio enthaltene Einzelrisiko gleichermaßen rückversichert ist, wird in der fakultativen Rückversicherung der Versicherungsschutz je Einzelrisiko separat verhandelt und abgeschlossen. In der Regel wird fakultative Rückversicherung für Risiken gekauft, die sich von dem üblichen Portfolio unterscheiden und somit nicht von dem bestehenden obligatorischen Rückversicherungsvertrag, zwischen dem Erstversicherer und dem Rückversicherer, erfasst sind. Aufgrund der hohen Individualität der Risiken von Industriever sicherungsnehmern, findet die fakultative Rückversicherung im Industriever sicherungsmarkt sehr viel mehr Anwendung als im Privatversicherungsmarkt (vgl. Pfeiffer 2000, S. 20 ff.).

Neben der Unterscheidung in fakultative und obligatorische Rückversicherung, erfolgt eine weitere Differenzierung von Rückversicherung in proportional und nichtproportional. Bei der proportionalen Rückversicherung erfolgt eine prozentuale Aufteilung des Risikos, diese Aufteilung findet bei der Prämie und dem Schaden Anwendung. Ausprägungen der proportionalen Rückversicherung sind die Quote, bei dem ein fester Prozentsatz für alle Risiken vereinbart wird, und der Summenexzedent, hier gilt für alle Risiken ein fester Selbstbehalt, aus dem sich die prozentuale Aufteilung ergibt. Zur nichtproportionalen Rückversicherung zählen die Schadenexzedenten pro Risiko und pro Ereignis sowie der Jahresüberschadenexzedent. Bei dieser Rückversicherungsart erfolgt eine Aufteilung des Schadens und nicht des Risikos. Festgelegte Prioritäten, welche der Erstversicherer trägt, und Haftstrecken werden als absolute Werte festgelegt, ohne eine Relation zum Einzelrisiko zu berücksichtigen. Die Priorität und Haftstrecke kann sich auf ein Risiko beziehen (Schadenexzedent pro Risiko), auf ein Ereignis (Schadenexzedent pro Ereignis) oder auf ein Jahr (Jahresüberschadenexzedent). Beide vorgenannten Ausprägungen von Rückversicherung werden im Gesamtversicherungsmarkt, ebenso wie im Industriever sicherungsmarkt, von Rückversicherern angeboten und von Erstversicherern, zum Zweck des Risikotransfers, gekauft (vgl. Pfeiffer 2000, S. 42 ff.).

16.5 Risikolandschaft von Industrikunden im Wandel – Implikationen für Industriever sicherer

Veränderungen in der Industrie und bei Unternehmen bedeuten auch für Industriever sicherer Veränderung – primär in Gestalt der damit verbundenen Risiken. Dabei können Megatrends wie Klimawandel, Globalisierung oder digitale Vernetzung Treiber sein. Oft stellen diese Veränderungen Risikoträger vor Herausforderungen, manche bieten aber auch neue Chancen. Drei aktuelle Trends und ihre Implikationen sollen zum Abschluss dieses Kapitels stehen und verdeutlichen, dass Industriever sicherung ebenso herausfordernd wie hochaktuell ist.

16.5.1 Globalisierung

Die zunehmende Vernetzung von Unternehmen und ihrer Produktions-, Liefer- und Absatzketten über nationale Grenzen hinaus führen seit Jahren zu tief greifenden Veränderungen in der Versicherung von Industrierisiken, etwa in der Sach-, Transport- oder Haftpflichtversicherung.

Multinationale Unternehmen sind mit Niederlassungen und Tochterunternehmen weltweit vertreten, sie produzieren und vertreiben ihre Produkte rund um den Globus und bilden Lieferketten über Länder und Kontinente hinweg. Die Internationalität der Geschäftsmodelle verändert die Risikosituation der Unternehmen und stellt hohe Anforderungen an den Versicherungsschutz. Das gilt für große, internationale Konzerne, aber auch für

erfolgreiche Mittelständler, die auf der Basis starker Wettbewerbspositionen international expandieren.

Um die internationale Risikobelegenheit bestmöglich abzusichern sind entsprechend internationale Versicherungsprogramme nötig. Durch sie ist es Industriever sicherern möglich, im besten Sinne globalen Versicherungsschutz zu bieten und Risiken weltweit zu steuern. Versicherungsprogramme verbinden individuelle, weltweit gültige Deckungskonzepte mit der Notwendigkeit lokaler Versicherungspolicen und einer Betreuung vor Ort. Das heißt: Durch das Installieren einer Masterpolice wird ein einheitlicher Versicherungsschutz für sämtliche Auslandseinheiten und zugehörige Unternehmen zentral dargestellt; um lokalen Besonderheiten und vor allem gesetzlichen Vorschriften nachzukommen und kleinere Schadenefälle unkompliziert vor Ort abwickeln zu können, werden in den einzelnen Ländern Lokal-Policen mit einem schmalen Deckungsumfang platziert. An diese knüpft die Masterpolice im Hinblick auf mögliche *Differences in Limits (DIL)* und *Differences in Conditions (DIC)* an. Ungleichheiten durch unterschiedliche Versicherungsstandards in den Ländern werden so ausgeglichen. Die gesetzliche Regelung *Freedom of Services (FoS)* bietet die Möglichkeit, Unternehmensdienstleistungen grenzüberschreitend innerhalb des Europäischen Wirtschaftsraums zu erbringen und damit Versicherungsverträge in einem anderen Land abzuschließen, als sich das Risiko befindet. Gilt Dienstleistungsfreiheit im Sinne des FoS müssen keine Lokalpolicen installiert werden.

Darüber hinaus ändern sich mit der Globalisierung Supply-Chain-Risiken, weil Unternehmen sich so Unterschiede in den Faktorkosten zunutze machen oder neue lokale Märkte erobern. Fundamentale Veränderungen in den Wertschöpfungsketten sind die Folge. Denn korrespondierend zu den Potenzialen erhöhen sich auch die Ausfall- und Unterbrechungsrisiken für die Unternehmen; mit den enormen Chancen werden auch die Risiken globaler. Unterbrechungen in der Lieferkette können zu Verlusten mit potenzieller Existenzbedrohung führen. Solche Verluste erleiden zeitgleich mehrere Unternehmen, wenn durch ein Schadenereignis nicht nur einzelne Unternehmen, sondern ganze Branchen betroffen sind. Für Versicherer erhöhen sich die Risiken, in der einzelnen Kette und im Kumulszenario. Insbesondere Naturgefahren stellen diesbezüglich eine besonders große Gefahr dar. Sie können ganze Regionen treffen, wodurch das Risiko besteht, dass verschiedene Unternehmen gleichzeitig die geforderten Zwischen- bzw. Teilprodukte nicht liefern können (vgl. Bruch und Münch 2018, S. 68).

Die Brisanz der Betriebsunterbrechung durch Ausfälle in der Wertschöpfungskette wird am Beispiel „Meridian“ deutlich. Durch die Lahmlegung eines Produktionsstandortes des amerikanischen Automobilzulieferers „Meridian Magnesium Products“ in Folge einer Explosion im Mai 2018 waren verschiedene Automobilhersteller mit Lieferengpässen konfrontiert. Das Unternehmen stellt für die Automobilhersteller Cockpit-Querträger her. Durch den Schaden konnte Meridian die geforderten Bestellmengen nicht liefern. Dies hatte eine starke Einschränkung der Produktion bei den Automobilherstellern zur Folge (vgl. Hubik 2018).

Zusammenfassend lässt sich sagen, dass in dem Maße, in dem die deutsche Wirtschaft expandiert, nicht nur die Bedeutung internationaler Programme zunehmen; auch die

Mächtigkeit des Schutzes selbst nimmt signifikant zu. Deutlich wird auch, wie hoch der fachliche Anspruch an das Produkt Industriever sicherung durch Globalisierung wird. Denn es gilt, internationale Netzwerke aufzubauen und fachliche Expertise rund um den Globus zur Verfügung zu stellen. Der Versicherungsmarkt selbst erfährt einen Globalisierungsprozess. Die großen und führenden Versicherungsunternehmen sind mittlerweile in fast allen Ländern lokal vertreten. Es ist interessant, dass die Expansion gerade deutscher Versicherungsunternehmen wie der Allianz oder des HDI untrennbar verbunden ist mit einer global handelnden deutschen Industrie. Wer in der Lage ist, die hohen Eingangshürden zu nehmen, dem stehen mit der Industriever sicherung hochinteressante Märkte und Chancen offen.

16.5.2 Digitalisierung und Vernetzung

Wir leben im Zeitalter der vierten industriellen Revolution (Industrie 4.0). Digitalisierung und Sensorik ermöglicht die Vernetzung sämtlicher Unternehmens- und Lebensbereiche. Der digitale Wandel wird immer schneller und ist noch weit davon entfernt, sein Maximum erreicht zu haben. In den letzten Jahren sind Umbrüche in der Gesellschaft, für Unternehmen wie jeden einzelnen zu spüren, weitere werden folgen. So stehen Durchbrüche und die hieraus resultierende Verbreitung in den Bereichen der autonomen Mobilität, der künstlichen Intelligenz und dem Internet der Dinge kurz vor der Umsetzung. Die sich durch die Digitalisierung ergebenden Umweltveränderungen erfordern ständige Veränderung. Unternehmen müssen sich in einer volatilen, unsicheren, komplexen, uneindeutigen Welt behaupten (vgl. Kollmann und Schmidt 2016, S. 162 ff.). Mit den Veränderungen für die Industrie gehen große Änderungen der Risiken einher, welche durch Industriever sicherer abgesichert werden. Die Industrie 4.0 erfordert demzufolge auch eine „Versicherung 4.0“, da die alten Standardprodukte der Versicherungsbranche nicht mehr ausreichen, um Unternehmen in Zeiten des digitalen Wandels adäquaten Versicherungsschutz zu bieten. Traditionelle Verfahren für die Kalkulation der Risiken sind nur mehr eingeschränkt auf neue Risiken anwendbar, Muster wollen und müssen erst erkannt werden. Neue Ansätze zur Risikobewertung bei den Industriever sicherern müssen entwickelt und implementiert werden (vgl. BDI 2019).

Hinzu kommt, dass immaterielle Vermögenswerte, vordergründig Daten, aber auch Netzwerke, Plattformen oder Markenwerte, mit der Virtualisierung unserer Welt an Bedeutung und Wert für Unternehmen gewinnen. So ergibt sich eine veränderte Vermögensstruktur, die auch bei traditionellen Industrieunternehmen zu beobachten ist. Im Vergleich mit den haptischen Fertigungsprodukten werden zunehmend große Gewinnanteile durch digitale Produkte und Dienstleistungen erwirtschaftet. Für Risikomanager, Intermediäre wie Versicherer nehmen die schwer messbaren, immateriellen Vermögenswerte der Unternehmen rasant an Bedeutung zu (vgl. Bruch und Münch 2018, S. 64 f.).

Neuartige Risiken erfordern für die Industriever sicherer andere Ansätze im Underwriting. Basierte dieses bisher auf den Schadenerfahrungen vergangener Jahre, auf

Erfahrungswerten und der Einschätzung von Experten, verändern Big-Data-Analysen, zukunftsfockussierte Modellierungen und mittels künstlicher Intelligenz lernende Algorithmen die Möglichkeiten die Zukunft des Underwritings radikal. Es wird datengetrieben, parametrische Lösungen breiten sich aus. Noch gilt, dass das klassische Underwriting durch modernen Techniken unterstützt wird; Technik hilft, neue Risiken und bekannte Risiken neu einschätzen und tarifieren zu können, sie unterstützt bei der Portfoliosteuerung und kann ein Faktor sein, mittels dessen sich Industriever sicherer differenzieren und abheben (vgl. Bruch und Münch 2018, S. 69 f.).

Offen ist, ob und wie lange das so bleibt, wie lange es also braucht, bis die Technik ganz übernimmt. Studien gehen davon aus, dass 40 bis 50 Prozent aller Underwriter durch einen Robo-Underwriter ersetzt werden könnten. Auch und gerade in der Industriever sicherung.

16.5.3 Cyberrisiken und -versicherung

Mit der Digitalisierung von Prozessen gewinnt die IT-Struktur der Unternehmen, Daten und digitale Infrastrukturen nehmen immer mehr an Bedeutung zu. Durch die zentrale Rolle, die die IT im weitesten Sinne einnimmt, stellt sie auch ein besonders großes Gefahrenpotenzial und Angriffsziel im Falle eines Ausfalls dar, eine rasch wachsende man-made Gefahr, gezielt oder durch Fehler getrieben.

In diesem Umfeld exponentiell steigender Risiken und Schadenszenarien stellt die Cyber-Versicherung mehr als nur („mal wieder“) ein neues Versicherungsprodukt dar; sie hat das Potenzial, über das Produkt Risikotransfer hinaus einen neuen Versicherungszweig zu begründen und den Einstieg in die Ökosystem-Ökonomie zu forcieren. Ursprünglich aus den USA kommend, wird dieses Produkt seit 2011 in Deutschland angeboten. Nachdem der Bedarf für solche Versicherungslösungen anfangs nicht wahrgenommen wurde, ist spätestens mit der weltweiten Verbreitung von Verschlüsselungstrojanern wie „Wannacry“ die Nachfrage nach Cyber-Versicherungen deutlich angestiegen. Als Konsequenz entwickelten diverse Versicherer am Markt Produkte der Cyber-Versicherung, sodass aktuell ein breites Angebot zur Verfügung steht. Der Markt wächst.

Die klassische Cyberdeckung besteht aus den drei Deckungskomponenten Haftpflicht, Eigenschaden und Betriebsunterbrechung und stellt somit eine Multiriskdeckung dar. Im Haftpflichtbaustein wird grundsätzlich die Haftungsfrage geklärt, berechtigte Ansprüche sind vom Versicherungsschutz umfasst, während unberechtigte Ansprüche durch den Versicherer gegenüber dem Anspruchsteller abgewiesen werden. Während der Eigenschadensbereich Kosten umfasst, die durch die Beauftragung von zum Beispiel forensischen Untersuchungen anfallen können, deckt die Komponente der Betriebsunterbrechung sämtliche Kosten, die entstehen, wenn ein Unternehmen aufgrund einer Cyber-Attacke nicht mehr produktionsfähig ist. Die Cyberversicherung wird aufgrund dieser Besonderheiten der Sparte Financial Lines zugeordnet.

Neben allen Chancen stellt die Cyber-Versicherung Versicherer (wieder) vor Herausforderungen.

- Die Prämienkalkulation des Produktes Cyber ist schwierig. Es kann weder das potentielle Schadenausmaß wirklich kalkuliert, noch eine Schadenfrequenz präzise prognostiziert werden – zu klein sind noch Anzahl der bekannten Schäden und Daten hierüber. Gearbeitet wird mit Szenarien und jedem irgendwie verfügbaren Datum. Das für die Cyber-Versicherer damit entstehende Risiko ist nicht zu vernachlässigen.
- Aus Schadenerfahrungen resultiert die Erkenntnis, dass die durch die Cyber-Versicherung abgedeckten Schäden auch durch herkömmlichen Versicherungsschutz gedeckt sein können, dass für den Versicherer und seine Haftpflicht-, Sach- oder Spezialdeckungen ein „silent Cyber“ Risiko besteht. Im Schadenfall läuft der Versicherer Gefahr, für dasselbe Ereignis zweimal zu zahlen. Es beschreibt die Möglichkeit, dass ein Cyberangriff die Deckung einer Versicherung auslöst, obwohl dort ursprünglich dieses Risiko nicht berücksichtigt und somit auch nicht eingepreist wurde. Erste Versicherungsunternehmen haben vor diesem Hintergrund damit begonnen etwaige Cyberausschlüsse aufzunehmen oder einen Prämienzuschlag für dieses Risiko zu verlangen (vgl. Willis Tower Watson 2018).
- Nicht zuletzt entstehen aufgrund der spezifischen Struktur des Risikos für den Markt neue Kumulrisiken und -szenarien. Ungerichtete wie gezielt lancierte Schadsoftware etwa könnte Schadenereignisse rund um den Globus nach sich ziehen und damit viele Policen triggern.

Grundsätzlich lässt sich das Potenzial für den Markt für Cyberdeckungen nicht abschließend einschätzen – weder umsatz- noch ertragsseitig. Noch erzielen Versicherungsunternehmen dort gute Ergebnisse, sowohl beim Wachstum wie auch in der Combined-Ratio. Dennoch sind sie sich des Risikos bewusst, dass jederzeit ein Großschaden das Portfolio treffen – im Produkt Cyber wie auch „silent“ in anderen Sparten.

Dennoch steht Cyber abschließend einmal mehr für unsere These, dass auf dem hochinteressanten, aber auch anspruchsvollen Markt für Industriever sicherung immer wieder neue, spannende Chancen entstehen, wenn Versicherer gewillt sind, in Expertise und Know how zu investieren – und Risiken einzugehen.

Literatur

- Allianz Global Corporate & Specialty. (Hrsg.) (2018). Geschäftsbericht 2017, München.
- AXA SA. (2018) Risk Engineering. <https://axaxl.de/produkte-und-dienstleistungen/risk-engineering>. Zugegriffen am 31.07.2019.
- Banks, E. (2004). *Alternative Risk Transfer; Integrated Risk Management through Insurance, Reinsurance, and the Capital Markets*. West Sussex: Wiley Finance.
- BDI – Bundesverband der Deutschen Industrie e. V. (2019) Industrie 4.0 braucht Versicherung 4.0. <https://bdi.eu/artikel/news/industrie-4-0-braucht-versicherung-4-0-1/>. Zugegriffen am 31.07.2019.

- Bruch, M., & Münch, V. (2018). Neue Risiken – neues Underwriting. In A. Eckstein, A. Liebetrau & A. Funk-Münchmeyer (Hrsg.), *Insurance and Innovation 2018*. Karlsruhe: VVW.
- Brühwiler, B. (1994). *Internationale Industriever sicherung; Risk Management – Unternehmungsführung – Erfolgsstrategien*. Karlsruhe: VVW.
- CGE Risk Management Solutions. (2018). Conform to ISO 31000 using the bowtie method. <https://www.cgerisk.com/2018/06/conform-to-iso-31000-using-the-bowtie-method/>. Zugegriffen am 31.07.2019.
- Cummins, J. D., Doherty, N. A., Ray, G., & Vaughan, T. (2006). The insurance brokerage industry post-October 2004. *Risk Management an Insurance Review*, 9(2), 89–108.
- DIN Deutsches Institut für Normung e. V. (2019). DIN-Normenausschuss Organisationsprozesse (NAOrg) <https://www.din.de/de/mitwirken/normenausschuesse/naorg>. Zugegriffen am 31.07.2019.
- Eisen, R., Zweifel, P. (Hrsg.) (2013). *Versicherungsökonomie* (2. Aufl.). Heidelberg: Springer.
- Farny, D. (2011). *Versicherungsbetriebslehre* (5. Aufl.). Karlsruhe: VVW.
- Fromme, H. (2019). Ecclesia und Aon Kopf an Kopf. Herbert Frommes Versicherungsmonitor am 24.06.2019. <https://versicherungsmonitor.de/2019/06/24/ecclesia-und-aon-kopf-an-kopf/>. Zugegriffen am 25.02.2020.
- Fromme, H., & Hagen, P. (2019). Higher premiums in property insurance. Herbert Frommes Versicherungsmonitor Dossier No 12: Ferma 2019 Search for a new Relationship, November 2010, 6–9.
- GDV. (2019). Über uns. Versicherungsunternehmen. <https://www.gdv.de/de/ueber-uns/unsere-mitglieder/versicherungsunternehmen>. Zugegriffen am 31.07.2019.
- GDV. (2019a). Industriever sicherungen – Wie sich Unternehmen gegen Betriebsunterbrechungen absichern können. <https://www.gdv.de/de/themen/positionen-magazin/wie-sich-unternehmen-gegen-betriebsunterbrechungen-absichern-koennen-44162>. Zugegriffen am 20.11.2019.
- Gothaer Konzern (Hrsg.). (2018). *Aktuelles strategisches Thema 2018: Mehrwert durch Gemeinschaft*. Köln. https://heller.gothaer.de/media/ueber_uns_1/konzern/gesellschaften/gothaer_image-broschuere_2018.pdf.
- HDI Global SE. (2019). Talanx und HDI setzen sich ambitioniertere Ziele. <https://www.hdi.global/de/de/infocenter/hdi-infocenter/oktober-2018/artikel11>. Zugegriffen am 31.07.2019.
- Heep-Altiner, M., Mullins, M., & Rohlfs, T. (2018). *Solvency II in the Insurance Industry*. Cham: Springer.
- Hubik, F. (2018). In handelblatt.com. Daimler und Ford stoppen Produktion nach Brand bei US-Zulieferer. <https://www.handelsblatt.com/unternehmen/industrie/lieferengpaesse-daimler-und-ford-stoppen-produktion-nach-brand-bei-us-zulieferer/21263586.html?ticket=ST-3411618-XGe-aHafjqiwY2jxTuYLd-ap1>. Zugegriffen am 31.07.2019.
- Kollmann, T., & Schmidt, H. (2016). *Deutschland 4.0*. Wiesbaden: Springer.
- Mikosch, C. (2005). *Industriever sicherungen; Eine Führung durch den Versicherungsdschungel* (2. Aufl.). Wiesbaden: Springer.
- Pfeiffer, C. (2000). *Einführung in die Rückversicherung: das Standardwerk für Theorie und Praxis* (5. Aufl.). Wiesbaden: Gabler.
- Schaloske, H. (2013). *Folgerungen aus der Dornbracht-Entscheidung für die Praxis der offenen Mitversicherung*. Hamburg: VVW.
- Willis Tower Watson (Hrsg.). (2018). *Industriever sicherungen MARKTspot 2018 Rückblick I Ausblick*. Frankfurt. <https://www.willistowerswatson.com/-/media/WTW/Insights/2018/06/MARKTspot-2018-WEB.pdf?modified=20180618123335>.
- Zurich Gruppe Deutschland (Hrsg.). (o. J.). Zurich Versicherung Schützen Sie, was Sie wirklich lieben, Bonn.

Dr. Christopher Lohmann fand den Einstieg in die Versicherungsbranche als Vorstandsassistent bei der Allianz AG. Nach Stationen im Vertrieb, in Betrieb und Schaden sowie im Controlling übernahm Lohmann 2013 die Geschäftsführung der Allianz Global Corporate & Specialty SE, in Zentral- und Osteuropa. In der AGCS bündelt die Allianz ihr Geschäft mit Industriekunden sowie Spezialgeschäfte wie Luft- und Seefahrt. Im April 2017 trat Lohmann in den Gothaer Konzern ein. Als Vorstandsvorsitzender der Gothaer Allgemeine AG verantwortete er die gesamte Kompositversicherung des Konzerns im Inund Ausland sowie den Bereich Schaden; zudem war er Mitglied des Vorstands der Gothaer Versicherungsbank VVaG und der Gothaer Finanzholding AG. Seit August 2020 ist Lohmann als Vorstandsmitglied der Talanx AG sowie CEO des HDI Deutschland verantwortlich für den Privat- und Firmengeschäftsbereich des Konzerns in Deutschland.

Stefan Sowietzki begann seine Versicherungslaufbahn nach absolviert er Lehre und dem betriebswirtschaftlichen Studium an der Fachhochschule für Versicherungswesen 1994 beim Gerling-Konzern in Köln. Über Stationen in der Versicherungsabteilung der Mannesmann AG und dem Versicherungsmakler Marsh kam er 2010 zur AXA Corporate Solutions. Von 2014 bis 2017 arbeitete er für die AXA in China beim dortigen Joint Venture AXA Tianping und war als CEO für den Großkundenbereich verantwortlich. Aktuell leitet er den Konzernkunden-Vertrieb bei AXAXL in Deutschland.

Pauline Gewand studierte Business Administration mit dem Schwerpunkt Risiko- und Versicherungsmanagement an der Hamburg School of Business Administration. Parallel hierzu absolvierte sie eine Ausbildung zur Kauffrau für Versicherung und Finanzen bei der Funk Versicherungsmakler GmbH. Nach Abschluss des Bachelors arbeitete sie zwei weitere Jahre bei Funk in Hamburg. Zuletzt absolvierte sie das Masterstudium Risk & Insurance am Institut für Versicherungswesen der Technischen Hochschule Köln.



Holger Kraus und Julian Alexander Robles Häusser

Zusammenfassung

Der vorliegende Beitrag soll einen Überblick über Captives als Instrument der Finanzierung von versicherungsfähigen Risiken in Unternehmen geben. Hierzu werden insbesondere die Gründe für den Einsatz dieses Instrumentes, Fragestellungen im Zusammenhang mit Gründung und Betrieb und die wesentlichen Ausprägungsformen und ihre jeweiligen Charakteristika beleuchtet. Ziel ist es, ein grundsätzliches Verständnis zu vermitteln und eine erste Einschätzung zu ermöglichen, ob eine Captive in einer konkreten Unternehmenssituation eine prüfenswerte Option darstellt.

17.1 Einführung

Als Captives werden im Zusammenhang mit Versicherung selbstständige Rechtspersonen oder auch von Dritten gegen Gebühr zur Nutzung angebotene Infrastrukturen bezeichnet, die über die aufsichtsrechtliche Lizenz zum Betreiben des Erst- und/oder Rückversicherungsgeschäfts verfügen. Der Begriff „Captive“, mit der Bedeutung „gefangen“ oder „gefesselt“ röhrt daher, dass dieses Instrument zu einem Unternehmen gehört und von diesem betrieben wird, dessen Kerngeschäft sich außerhalb der Versicherungsindustrie befindet. Darüber hinaus weist diese Bezeichnung darauf hin, dass eine Captive in der Regel ausschließlich oder überwiegend für die Optimierung der Finanzierung von versiche-

H. Kraus (✉)

Siemens AG, München, Deutschland

E-Mail: holger.kraus@siemens.com

J. A. R. Häusser

TH Köln, Institut für Versicherungswesen, Köln, Deutschland

E-Mail: julian.robles@web.de

rungsfähigen Risiken, welche in engem Zusammenhang mit der originären Geschäftstätigkeit des Mutterunternehmens stehen, eingesetzt wird. Captives bilden damit vielfach einen integralen Bestandteil der Risikofinanzierungs- und Versicherungsstrategie von Unternehmen. Grundsätzlich können Captives auch Drittrisiken, das heißt Risiken, die in keinem Zusammenhang mit der Geschäftstätigkeit des Mutterunternehmens stehen, zeichnen (vgl. Fläming 2007, S. 54). Dies erfolgt in der Regel entweder, um zusätzliche Erlöse zu erzielen oder um die Anforderungen der Steuergesetzgebung am Sitz der Muttergesellschaft zu erfüllen, welche an die steuerliche Abzugsfähigkeit von an Captives bezahlten Prämien als Betriebsaufwand gestellt werden.

Die ersten Captives entstanden in Europa bereits in den 1920er-Jahren. Der Grund hierfür lag darin, dass kommerzielle Versicherer entweder fehlten und nicht willens waren, wichtige Risiken zu versichern. Beispiele hierfür waren die Captive von British Petroleum, namens „Tanker“, für „shipping risks“ (UK) oder die Captive von Imperial Chemical Industries‘ (ICI) für Transporte von explosiven Stoffen. Diese Captives wurden am Sitzland ihrer jeweiligen Mutter („onshore“) betrieben. Die erste Captive an einem heute klassischen „offshore“ Captive Standort wurde 1953 auf Bermuda gegründet (vgl. International Risk Management Institute 2019).

Weltweit bestanden per Ende 2018 ca. 6300 Captives (Ende 2017 ca. 6500) (vgl. Captive Review 2019). Damit setzt sich der leicht rückläufige Trend der vergangenen Jahre fort, welcher insbesondere auch auf Captive-Konsolidierungen in der Folge von Unternehmensübernahmen und -fusionen zurückzuführen ist. Unternehmen, welche über eine Captive verfügen, halten vielfach auch in Zeiten weicher Versicherungsmärkte an diesem Risikofinanzierungsinstrument fest.

Mit ca. 50 Prozent des Gesamtbestandes ist die Mehrzahl der Captives in den USA beheimatet. Es folgen mit 34 Prozent Bermuda und die Karibik, mit 13 Prozent Europa und mit drei Prozent die Region Asia-Pacific. In Afrika und im Mittleren Osten befindet sich lediglich ein Prozent der Captives (vgl. Captive Review 2019). Wesentliche Captive-Domizile in der Europäischen Union sind Luxemburg, Irland und Malta.

In Deutschland sind per Ende 2018 neun Captives beheimatet, davon drei mit einer Erstversicherungs- und sechs mit einer Rückversicherungslizenz. Alle unterliegen der Aufsicht durch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin).

17.2 Gründe für den Einsatz einer Captive

Grundsätzlich lassen sich zwei übergeordnete Gründe für den Einsatz einer Captive nennen: Die Optimierung der Finanzierung der versicherungsfähigen Risiken in einem Unternehmen und/oder die Generierung zusätzlicher Erlöse durch den Verkauf von Versicherung als Ergänzung zum Kernprodukt bzw. zur Kerndienstleistung des Unternehmens.

In der Mehrzahl der Fälle dürfte die Optimierung der Risikofinanzierung im Vordergrund stehen. Für international tätige Unternehmen oder Unternehmensgruppen ist es oft-

mals sinnvoll, über ein Instrument zu verfügen, welches die Bündelung weltweit belegener versicherbarer Risiken erlaubt und somit eine zentrale Entscheidung über Eigentragung und Transfer von Risiken an Dritte ermöglicht. Durch steuerliche und aufsichtsrechtliche Anforderungen kann diese Bündelung nur über eine Rechtsperson erfolgen, die zum Betrieb des (Rück-)Versicherungsgeschäfts befugt ist, da der Risikoausgleich im Kollektiv, das heißt über juristische Personen hinweg, in einer Vielzahl von Ländern als Versicherung klassifiziert und somit der jeweiligen lokalen Versicherungsaufsicht unterworfen ist. Das Betreiben einer nicht formalisierten „Familienkasse“, die von Tochterunternehmen Beiträge erhält bzw. im Schadenfall Entschädigungen an die Tochterunternehmen leistet, ist daher keine gangbare Alternative. Neben der zentralen Entscheidungsfindung unterstützt eine Captive die zeitnahe Verfügbarkeit qualitativ hochwertiger Schadeninformationen, welche wiederum als Grundlage für effektive Risikomanagementmaßnahmen genutzt werden können. Dieser Umstand wird in der Captive-Literatur oftmals nicht genannt, obwohl er einen wertvollen Vorteil darstellt.

Darüber hinaus ermöglichen Captives eine individuelle Anpassung des Versicherungsumfanges an den Bedarf der einzelnen operativen Einheiten innerhalb einer Unternehmensgruppe (ggf. auch aufgrund entsprechender Kundenanforderungen) sowie einen Ausgleich zwischen der Risikotragfähigkeit der einzelnen Tochterunternehmen und des Gesamtunternehmens. So können den Tochterunternehmen ihrer jeweiligen Finanzkraft entsprechende Selbstbehalte zur Verfügung gestellt werden und gleichzeitig auf Gesamtunternehmensebene eine der Gesamtrisikotragfähigkeit angemessene Eigentragung umgesetzt werden. Dadurch können zusätzliche Prämienaufwände der Tochterunternehmen zum Beispiel infolge lokalen Erwerbs von Versicherungsschutz oder „Herunterkaufens“ von als zu hoch erachteten Selbstbehalten vermieden werden. Darüber hinaus kommen Captives auch bei Risiken zum Einsatz, die im Versicherungsmarkt nicht oder nur teilweise oder – aus Sicht des Versicherungsnehmers – nur zu unangemessenen Konditionen versichert werden können. Vor allem wenn es zu technischen Schwierigkeiten bei der Beurteilung des Risikos kommt, zum Beispiel bei neuen Technologien, neuen Märkten etc., kann über die Beteiligung einer Captive die Verfügbarkeit von Risikotransfer ermöglicht werden.

Die Möglichkeit einer zentralen Entscheidung darüber, welche Risiken im Unternehmen verbleiben sollen und welche Risiken an Versicherer oder Rückversicherer transferiert werden sollen, eröffnet dem Unternehmen einen deutlich höheren Handlungsspielraum in der Ausgestaltung der Finanzierung von versicherungsfähigen Risiken und der Interaktion mit dem Versicherungsmarkt. Die Captive stellt somit eine Realoption dar, die es ermöglicht, die Risikoeigentragung strategisch und ein Stück weit unabhängig vom Versicherungsmarkt zu tätigen oder aber die Gesamtrisikokosten kurzfristig zu optimieren.

Im Rahmen der Konzernrisikoeigentragung werden Captives vielfach im Bereich hoher bis mittlerer Schadenfrequenz und geringer bis mittlerer Schadenhöhe eingesetzt. Dies dient dem Ziel, Geldwechselgeschäfte mit Versicherern zu vermeiden und auf die der Cap-

tive zufließenden Prämienanteile Gemeinkosten oder Gewinnaufschläge, welche der Versicherer im Transferfall in Ansatz bringt, einsparen zu können. Die Kostenquote für die Finanzierung erwarteter Schäden mit ihrer überschaubaren Volatilität kann somit optimiert werden.

Darüber hinaus verbleiben die an eine Captive fließenden Prämienanteile bis zur Verwendung für die Auszahlung von Schäden im Unternehmen. Die Mittel können in diesem Zeitraum in verschiedenen Kapitalanlageinstrumenten investiert werden, um damit Anlagerträge zu generieren (vgl. Ilić 2012, S. 46 f.) oder, sofern und soweit dies die aufsichtsrechtlichen Regelungen am Standort der Captive zulassen, auch unternehmensintern, zum Beispiel für einen Kredit an die Muttergesellschaft verwendet werden. Die Erträge aus den Kapitalanlagen und ihre Signifikanz für die Wirtschaftlichkeitsbetrachtung einer Captive sind einerseits von der Kapitalanlagestrategie und andererseits von Kapitalmarktfeld und Zinsniveau geprägt. Da die Kapitalanlagen von Captives vielfach konservativ ausgerichtet sind und zu großen Teilen aus festverzinslichen Wertpapieren und Bankeinlagen bestehen, kommt den Kapitalerträgen in Niedrigzinsphasen in der Regel eine eher untergeordnete Rolle zu.

Zudem bieten Captives einen direkten Zugang zum Rückversicherungsmarkt. Dies eröffnet die Möglichkeit, Unterschiede in der Bepreisung von Risiken zwischen Erst- und Rückversicherungsmarkt zu identifizieren und zum Vorteil des Unternehmens zu nutzen. So kann eine Captive zum Beispiel im Rahmen eines internationalen Versicherungsprogrammes vom führenden Versicherer nur den Risikoanteil übernehmen, der letztlich auch in der Captive verbleiben soll (Nettozession) oder aber das Risiko zunächst vollständig übernehmen (Bruttozession) und die Risikoanteile, die nicht in der Eigentragung verbleiben sollen, bei geeigneten Rückversicherern platzieren (Retrozession).

Der zweite wesentliche Grund, aus welchem Captives eingesetzt werden, ist die Generierung zusätzlicher Erlöse durch den Verkauf von Versicherungen als Ergänzung zu dem/der von der Muttergesellschaft der Captive angebotenen Kernprodukt oder Kerndienstleistung.

Ein Beispiel hierfür ist die Telefónica Insurance S. A., eine luxemburgische Versicherungsgesellschaft mit Zulassung zum Versicherungsbetrieb in Deutschland, Spanien, Großbritannien und anderen Ländern der Europäischen Union. Die Telefónica Insurance S. A. wurde im Dezember 2004 gegründet und gehört zu der Telefónica Gruppe. Telefónica Insurance S. A. zeichnet Versicherungsdeckungen für Mobiltelefone, welche Kunden von Telefónica im Zusammenhang mit dem Abschluss von Mobilfunkverträgen erwerben. Die Deckung bietet eine Absicherung neuer Smartphones gegen Diebstahl, Herunterfallen oder Feuchtigkeitsschäden (vgl. Telefónica Insurance S. A. 2017). Weitere Einsatzfelder sind Produktschutzdeckungen oder Gewährleistungsverlängerungen. Gegenüber externen Versicherern verfügen hier die Captives über deutlich bessere Risikoinformationen und haben damit eine sehr gute Basis für die Abschätzung des zu erwartenden Schadenaufwands und die Prämienkalkulation.

17.3 Fragestellungen im Zusammenhang mit Gründung und Betrieb

Abklärung der Machbarkeit

Im Zusammenhang mit der Gründung einer Captive stellt sich eine Vielzahl von Fragen. Um einen effizienten Prüfungsprozess zu ermöglichen, bietet sich ein zweistufiges Verfahren an. In einem ersten Schritt ist es sinnvoll, zum einen eine Abschätzung der Wirtschaftlichkeit vorzunehmen und zum anderen die Einschätzungen und ggf. Vorbehalte wesentlicher Anspruchsgruppen im Unternehmen aufzunehmen.

Die Wirtschaftlichkeitsabschätzung erfolgt auf Basis einer Geschäftsplanung für die durch die Captive vorgesehene Risikoübernahme mit den wesentlichen Komponenten versicherungstechnisches Ergebnis, Kapitalanlageergebnis und Betriebskosten. Zeigt diese Erstabschätzung ein positives Ergebnis, empfiehlt sich die Einbindung wesentlicher Anspruchsgruppen im Unternehmen, wie die Bereiche Recht, Steuer, Treasury, Controlling/ Rechnungswesen und ggf. weitere, um frühzeitig Anforderungen und mögliche Hindernisse bzw. Widerstände zu identifizieren. Die zu adressierenden Themenfelder beginnen bei der aktuellen Unternehmensmeinung bezüglich der Neugründung von Tochtergesellschaften und gehen über die Einschätzung von regulatorischen und steuerlichen Themen und ggf. Risiken bis zu Fragen der Verfügbarkeit von Kapital und der Bereitschaft zur ggf. erforderlichen Sicherheitseinstellung gegenüber frontenden Versicherern (Zedenten). Sofern sich aus diesen Themenfeldern keine unüberwindbaren Hindernisse ergeben, empfiehlt es sich, eine Machbarkeitsstudie zu erstellen, in der alle für die Entscheidung relevanten Themenfelder detailliert analysiert und bewertet werden und an deren Ende eine konkrete Handlungsempfehlung und die Beschreibung des Durchführungsweges stehen. Wesentliche Inhalte der Machbarkeitsstudie sind ein detaillierter Geschäftsplan inkl. Sensitivitätsanalyse, die Evaluation des geeigneten Instruments sowie die Evaluation des geeigneten Standortes. Ein solcher Prozess kann je nach Art und Umfang einige Monate dauern (vgl. Erdmann 2017, S. 14).

Detaillierter Geschäftsplan

Die Erstellung eines mehrjährigen Geschäftsplanes bildet die Basis für die Analyse der Wirtschaftlichkeit eines Eigentragungsinstruments. Im Rahmen der Geschäftsplanung werden versicherungstechnisches Ergebnis, Erträge aus Kapitalanlagen und Betriebskosten im Detail geplant.

Grundlage für die Planung des versicherungstechnischen Ergebnisses bilden das erwartete Prämievolumen sowie der erwartete Schadenaufwand je Sparte. Das erwartete Prämievolumen kann über die seitens der Versicherer für eine höhere Eigentragung erwartete Rabattierung der aktuellen Risikotransferprämie oder (bei Verfügbarkeit aussagekräftiger Schadendaten) über eine aktuarielle Modellierung des erwarteten Schadenaufwands zuzüglich eines Risikozuschlages ermittelt werden. Diese aktuarielle Modellierung erlaubt neben dem im Durchschnitt

zu erwartenden Schadenaufwand auch den Aufwand bei positivem oder negativem Risikoverlauf zu ermitteln. Somit kann sowohl der Erwartungswert des versicherungstechnischen Ergebnisses als auch die Sensitivität des versicherungstechnischen Ergebnisses in Abhängigkeit vom Schadenverlauf bestimmt werden.

Die Grundlage für die Planung der Erträge aus den Kapitalanlagen bildet die Kapitalanlagestrategie in Verbindung mit Betrag und Dauer der anzulegenden Mittel. Im aktuellen Marktumfeld ist bei entsprechendem Anspruch an Liquidität und Sicherheit ein positiver Anlageertrag nicht in jedem Fall realisierbar.

In einem weiteren Schritt erfolgt die Planung der Betriebskosten, welche insbesondere Personalkosten (bei Management mit eigenem Personal), Kosten für externe Dienstleister (zum Beispiel Captive-Manager, Aktuar, Wirtschaftsprüfer etc.) sowie Kosten für die Aufsicht umfassen.

Der Saldo aus versicherungstechnischem Ergebnis, Kapitalerträgen und Betriebskosten bildet das Vorsteuerergebnis und erlaubt eine Abschätzung der Wirtschaftlichkeit. Für die Bewertung des Ergebnisses ist es von Relevanz, ob die Captive als Cost-Center oder als Profit-Center geführt werden soll, das heißt, wie stark eine Gewinnerzielungsabsicht im Vordergrund steht.

Evaluation des geeigneten Instruments

Die Evaluation des geeigneten Instruments beantwortet insbesondere folgende Fragen:

Fragen

Frage 1: Soll die Risikoeigentragung über eine konzerneigene als Erst- oder Rückversicherungsgesellschaft lizenzierte Tochtergesellschaft oder mittels Nutzung einer bestehenden, von einem Versicherer oder einer anderen Gesellschaft angebotenen Infrastruktur gegen Gebühr (Rent-a-Captive oder Protected Cell Company) erfolgen?

Zur Beantwortung dieser Frage bietet es sich an, die Betriebskosten der verschiedenen Instrumente zu analysieren, den Umfang der Kapitalbindung zu vergleichen, den relevanten Zeithorizont zu bestimmen und Faktoren wie Flexibilität bzw. Unabhängigkeit zu bewerten.

Grundsätzlich werden die Gründung und der Betrieb einer eigenen Versicherungsgesellschaft mit höheren Kosten verbunden sein als die Nutzung einer bestehenden Infrastruktur eines Versicherers oder einer Protected Cell Company. Eine eigene Versicherungsgesellschaft ist mit dem regulatorisch geforderten Kapital auszustatten, das heißt, das Mutterunternehmen einer Captive muss bereit sein, Kapital in einer Tochtergesellschaft, welche nicht im Kerngeschäft des Unternehmens tätig ist, zu binden. Bei Nutzung einer „Rent-a-Captive“ oder einer Protected Cell Company ist das Einbringen von Kapital vielfach nicht oder nur in geringem Umfang erforderlich, da das Kapital vom Anbieter der Infrastruktur vorgehalten wird und eine Sicherheit durch den Infrastrukturnutzer zum Beispiel in Form einer Bankgarantie oder einer Bürgschaft ausreichend ist. Weiter relevant ist

der Umstand, wie schnell das Eigentragungsinstrument zur Verfügung stehen soll und für welchen Zeitraum die Nutzung vorgesehen ist. Grundsätzlich ist anzumerken, dass die Gründung und auch Abwicklung einer eigenen Versicherungsgesellschaft aufgrund gesellschaftsrechtlicher und aufsichtsrechtlicher Anforderungen und Prozesse deutlich mehr Zeit in Anspruch nehmen, als die Nutzung eines Rent-a-Captive oder einer Protected Cell Company. Im letzteren Fall sind lediglich vertragliche Vereinbarungen mit dem Infrastrukturbieter zu treffen. Die entsprechenden Prozesse und Dokumente sind weitgehend standardisiert, so dass sowohl die Implementierung als auch die Beendigung innerhalb weniger Monate realistisch ist. Darüber hinaus ist die Bedeutung von Flexibilität und Unabhängigkeit zu bewerten. In einer eigenen Versicherungsgesellschaft bestimmen die Organe im Rahmen der rechtlichen Rahmenbedingungen den Kurs und die Prozesse der Gesellschaft, bei der Nutzung einer bestehenden Infrastruktur sind diese Freiheitsgrade eingeschränkt, da hier zusätzlich die Anforderungen bzw. Restriktionen, die der Infrastrukturbieter auch zu seinem eigenen Schutz definiert, einzuhalten sind.

Fragen

Frage 2: Soll die Risikoeigentragung als Erstversicherung oder als Rückversicherung ausgestaltet werden?

Für die Beantwortung dieser Frage stehen die Belegenheit der Risiken, die Unterschiede in den aufsichtsrechtlichen Anforderungen, die Bedeutung des Frontings und die Betriebskosten im Vordergrund.

Die Belegenheit der zu versichernden Risiken ist insofern von Bedeutung, als das Domizil einer Erstversicherungsgesellschaft bestimmt, in welchen Ländern Risiken direkt gezeichnet werden können. Eine Erstversicherungscaptive ist insbesondere dann prüfenswert, wenn substantielle Teile der zu versichernden Risiken auch direkt gezeichnet werden können, das heißt, sich beispielsweise der Sitz der Captive in der EU befindet und gleichzeitig wesentliche Risiken in der EU belegen sind. Die aufsichtsrechtlichen Anforderungen an eine Direktversicherungsgesellschaft sind in der Regel höher als die an eine Rückversicherungsgesellschaft, da hier der Schutz des Versicherungsnehmers (auch wenn dies letztendlich die Muttergesellschaft der Captive ist) einen höheren Stellenwert einnimmt als bei Rückversicherungsgesellschaften, die ausschließlich mit entsprechend zugelassenen Erstversicherern kontrahieren.

Ein weiteres Themenfeld ist das Fronting. Eine Erstversicherungscaptive kann dem Versicherungsnehmer gegenüber (sofern er in einem von ihrer Lizenz umfassten Land domiziliert ist) direkt Versicherungspolicen ausstellen und benötigt dementsprechend keinen vorzeichnenden Versicherer oder Fronter. Auch die Schadenbearbeitung und -auszahlung kann direkt erfolgen. Eine Rückversicherungscaptive kann dies nicht. Hier übernimmt der Fronter die Policierung und die Schadenbearbeitung und -auszahlung. Der Fronter erhebt für seine gegenüber der Rückversicherungscaptive erbrachten Dienstleistungen und die Tragung des Gegenparteirisikos (der Fronter muss auch für vollständig

rückversichertes Geschäft aufsichtsrechtlich gefordert Risikokapital vorhalten, wobei die Höhe von der Finanzkraft bzw. dem Rating der Captive abhängt) sogenannte Frontinggebühren. Darüber hinaus machen Versicherer in Abhängigkeit von Zessionsvolumen und Finanzstärke der jeweiligen Rückversicherungscaptive die Stellung von Sicherheiten zur Bedingung. Frontinggebühren und das Thema Sicherheitseinstellung entfallen bei einer Erstversicherungscaptive. Gleichzeitig muss aber eine Erstversicherungscaptive den Policierungs- und Schadenabwicklungsprozess bedienen und kann dies entweder mit eigenem Personal oder durch Einkauf bei einem Dienstleister sicherstellen. In der Analyse der Betriebskosten ist folglich zu prüfen, ob eine Erstversicherungscaptive oder eine Rückversicherungscaptive bei den Aufwendungen für den Versicherungsbetrieb insgesamt günstiger abschneidet.

Evaluation des geeigneten Standortes

Eine weitere wichtige Fragestellung betrifft den geeigneten Standort für eine Captive. Hierbei spielen sowohl quantitative als auch qualitative Aspekte eine Rolle, von der Belegenheit der Risiken (insbesondere bei Erstversicherungscaptives), über die Infrastruktur, aufsichtsrechtliche und steuerliche Rahmenbedingungen und Kosten des Betriebs bis hin zu Reputation.

Grundsätzlich ist zwischen einer Ansiedlung der Captive im Sitzland der Muttergesellschaft („onshore“) und einer Ansiedlung an einem klassischen Captive-Standort außerhalb des Sitzlandes der Muttergesellschaft („offshore“) zu unterscheiden.

Die Belegenheit der Risiken ist insbesondere bei Erstversicherungscaptives ein bestimmendes Kriterium für die Standortwahl. Der Standort muss so gewählt sein, dass die Direktzeichnung der Zielrisiken aufsichtsrechtlich zulässig ist. Sollen beispielsweise in der EU belegene Risiken versichert werden, ist für die Captive ein EU-Standort zu wählen, da bei einem Standort außerhalb der EU keine Direktzeichnung in EU-Länder möglich ist.

Auch die in einem Land vorhandene Infrastruktur für Captives, von Anbietern für Captive-Management-Dienstleistungen, über Anbieter von Protected Cells bis hin zu Anbietern spezifischer, für Captives relevanter Services, stellt ein wesentliches Entscheidungskriterium dar.

Besteht die Intention, eine Protected Cell Lösung zu implementieren, ist die Zahl der Standorte weltweit stark begrenzt, da nur in ausgewählten Ländern ein entsprechender gesetzlicher Rahmen besteht und dieses Instrument nur in diesen Ländern zur Verfügung steht. Die erste Zulassung einer Protected Cell Company erfolgte am 01.02.1997 auf der britischen Kanalinsel Guernsey. Als weitere wesentliche Standorte sind Gibraltar, Malta, Bermuda und Vermont zu nennen.

Soll das Captive Management extern eingekauft werden, ist das Vorhandensein einer entsprechenden Infrastruktur Voraussetzung. So existiert weltweit eine Vielzahl klassischer Captive-Domizile, wie zum Beispiel Bermuda, Vermont, Guernsey, Luxemburg oder Dublin, an denen unabhängige oder zu den großen Maklerhäusern gehörige Captive Manager vertreten sind. Diese bieten Dienstleistungen an, welche ein quasi vollständiges

Outsourcing des Captive-Betriebes ermöglichen. Anders stellt sich die Situation derzeit in Deutschland dar: Hier besteht keine Infrastruktur für vollumfängliche Captive-Management Dienstleistungen. Das Captive-Management muss also eigenständig erfolgen, bzw. benötigte Dienstleistungen müssen individuell bei unterschiedlichen Anbietern eingekauft werden. Auch das Executive Management der Captive ist in der Regel vom Mutterunternehmen zu stellen und hat die entsprechenden Anforderungen der Aufsicht hinsichtlich persönlicher Zuverlässigkeit und fachlicher Eignung („fit & proper“) zu erfüllen.

Auch die aufsichtsrechtlichen und steuerlichen Rahmenbedingungen spielen eine nicht unerhebliche Rolle bei der Standortwahl. Das am jeweiligen Standort zur Anwendung kommende Aufsichtsrecht hat zum Beispiel über Kapitalanforderungen, Anforderungen an Organe und Berichts- und Dokumentationspflichten einen erheblichen Einfluss auf die Gründung, den Betrieb und eine mögliche Auflösung der Gesellschaft und damit auch auf die Betriebskosten.

Captives mit Sitz in einem der EU zugehörigen Land unterliegen dem aktuellen Aufsichtsrahmen Solvency II. Das EU-Projekt wurde ins Leben gerufen, um widersprüchliche Handlungsvorschriften für den Versicherungssektor zu verhindern. Dabei wurde Solvency II in Anlehnung an Basel II, welches die Solvenzregeln für den Banksektor vorschreibt, ins Leben gerufen. Grundlage von Solvency II ist das Dreisäulen-Modell (vgl. Auras 2017, S. 3).

Die drei Säulen unterteilen sich dabei in die quantitativen Anforderungen, die qualitativen Anforderungen sowie die Marktdisziplin und Transparenz. Die quantitativen Anforderungen befassen sich mit der Bewertung der Eigenmittel und der Bestimmung des Risikokapitalbedarfs. Im Mittelpunkt steht somit die Risikotragfähigkeit des Unternehmens. Die qualitativen Anforderungen bestehen aus den Anforderungen an die Ausgestaltung der Organisationsstruktur, von Kontrollfunktionen und des Risikomanagementsystems. Daneben wird hier auch der aufsichtsrechtliche Überprüfungsprozess geregelt. Im Rahmen der Marktdisziplin und Transparenz wird die Berichterstattung der risikorelevanten Sachverhalte systematisiert. Dabei sind Berichte und Meldeformulare zu unterscheiden; auch gibt es verschiedene Adressatenkreise (Öffentlichkeit und BaFin) für die bereitzustellenden Informationen (vgl. Rohlfs 2018, S. 88 f.).

Die konkreten aufsichtsrechtlichen Anforderungen an einem Captive-Standort innerhalb der EU ergeben sich aus unmittelbar wirksamem EU-Recht (Delegierte Verordnung, technische Standards) sowie den jeweiligen nationalen Gesetzen (zum Beispiel Versicherungsaufsichtsgesetz (VAG) in Deutschland) ergänzt um weitere Konkretisierungen der jeweiligen nationalen Versicherungsaufsicht (in Deutschland zum Beispiel Auslegungsentscheidungen der Bundesanstalt für Finanzdienstleistungsaufsicht, BaFin).

Mit Inkrafttreten von Solvency II haben sich für Versicherer und Rückversicherer neue und zum Teil deutlich erhöhte Anforderungen bzgl. der Berechnung und der Ausstattung mit Eigenmitteln, bzgl. der Geschäftsprozesse und ihrer Dokumentation sowie des Berichtswesens an die Öffentlichkeit und die Aufsicht ergeben. Dies führt dazu, dass Grün-

dung und Betrieb einer Captive unter Solvency II tendenziell aufwendiger und damit kostenintensiver geworden sind und sich damit die Wirtschaftlichkeitsschwelle für den Einsatz dieses Instruments zum Beispiel bezogen auf das Mindestprämienvolumen nach oben verschoben hat (vgl. Fläming 2007, S. 75). Dies ist der Fall, obwohl das in Solvency II verankerte Prinzip der Proportionalität vorsieht, dass die aufsichtsrechtlichen Anforderungen nach Art, Umfang und Komplexität der Risiken des Unternehmens angemessen zu erfüllen sind. Zur Umsetzung des Proportionalitätsprinzips gehen die Ansichten von Aufsicht und beaufsichtigten Unternehmen derzeit noch deutlich auseinander (vgl. Grund 2017, S. 7 und Auras 2017, S. 4). Darüber hinaus ist eine europaweit einheitliche Anwendung von Solvency II noch nicht zu beobachten. Daher bietet es sich an, bei Sitzwahl in der EU die konkreten Anforderungen am jeweils in Frage kommenden Standort im Detail zu analysieren und zu bewerten.

Captives mit Sitz außerhalb der EU unterliegen den am jeweiligen Standort geltenden lokalen Aufsichtsregelungen. Diese orientieren sich zum Teil an Solvency II, liegen zum Teil jedoch auch deutlich darunter mit entsprechender Auswirkung auf die Höhe der aufsichtsrechtlich begründeten Aufwendungen im Zusammenhang mit dem Betrieb der Captive. Für den Fall, dass eine nationale Aufsicht innerhalb der EU die Regulierung am Standort der Captive nicht als gleichwertig zu Solvency II einstuft, wird der Rückversicherungsschutz, den eine an einem entsprechenden Standort domizierte Captive gegenüber einem in der EU angesiedelten Fronting-Versicherer gibt aufsichtsrechtlich gegebenenfalls nicht vollständig anerkannt. Dies kann zur Folge haben, dass der Fronting-Versicherer die Captive als Rückversicherer ablehnt, zusätzliche Sicherheiten und/oder höhere Frontinggebühren fordert.

Auch die Steuergesetzgebung am Standort der Captive bzw. die steuerliche Qualifizierung des Captive-Domizils in der Steuergesetzgebung des Standorts der Captive-Muttergesellschaft ist bei der Standortwahl zu berücksichtigen. Ein sehr niedriger Steuersatz am Captive-Standort kann zum Beispiel dazu führen, dass die Gewinne der Captive nach den Vorgaben des Steuerrechts am Sitz der Captive Muttergesellschaft zu ermitteln sind (Beispiel: Außensteuergesetz in Deutschland). Die OECD hat im Rahmen ihres BEPS (Base Erosion and Profit Shifting)-Projektes Captives als mögliche Instrumente im Rahmen von Steuervermeidungsstrategien identifiziert. Entsprechend sind zukünftig höhere Anforderungen an Captives zu erwarten, um nicht als Steuervermeidungsinstrument klassifiziert zu werden, insbesondere in den Bereichen finanzielle Lage der Captive, kommerzielle Vorteile, die sich aus der Captive ergeben, Alternativen, die sich dem Captive-Eigentümer zum Einsatz der Captive bieten, Substanz der Captive, Prämienfindung und Transferpreisgestaltung und Standort der Captive (vgl. Willis Tower Watson 2016).

Alle genannten Faktoren wirken sich auf die Kosten des Betriebs einer Captive aus und sind damit entsprechend quantifizierbar. Sie spielen damit eine wesentliche Rolle für die Entscheidung hinsichtlich des Standortes. Als nicht quantifizierbarer Faktor tritt die Reputation des Standortes hinzu, das heißt, die Frage, ob aus dem Bekanntwerden des Betreibens einer Captive an einem bestimmten Standort mögliche Reputationsrisiken für die Muttergesellschaft resultieren können.

17.4 Wesentliche Ausprägungsformen

Um im Rahmen eines Risikotransfers Captive-Lösungen zu erreichen, bieten sich verschiedene Möglichkeiten der Ausgestaltung an (vgl. Palmberger 2016, S. 6).

Im Folgenden werden die wesentlichen Optionen beschrieben und einander anhand folgender Dimensionen gegenübergestellt.

- Eigene Tochtergesellschaft vs. Nutzung einer bestehenden Infrastruktur (Rent-a-Captive, Protected Cell Company)
- Erstversicherung vs. Rückversicherung
- Ein Eigentümer (Single Parent Captive) vs. mehrere Eigentümer (Multi Parent Captive)
- Eigenrisikotragung (Pure Captive) vs. Drittgeschäft (Broad oder Open Market Captive)

17.4.1 Eigene Tochtergesellschaft vs. Nutzung einer bestehenden Infrastruktur

Eine Captive kann entweder über eine rechtlich selbstständige Tochtergesellschaft oder aber über eine vertragliche Vereinbarung über die Nutzung einer bestehenden Infrastruktur umgesetzt werden.

Captive als eigene Tochtergesellschaft

Die Captive als eigene Tochtergesellschaft kann entweder mittels Gründung und Lizenzierung oder über den Erwerb einer bereits bestehenden Captive-(Rück-)Versicherungsgesellschaft erfolgen. Für Captive-Versicherungs- bzw. Rückversicherungsunternehmen bestehen sowohl durch die aufsichtsrechtlichen Rahmenbedingungen am Standort der Captive sowie durch (steuer-)rechtliche Rahmenbedingungen am Sitz der Muttergesellschaft definierte Mindestanforderungen zum Beispiel hinsichtlich Kapitalisierung und Geschäftsorganisation. Aufgrund des damit einhergehenden Aufwandes ist die Gründung und der Betrieb einer eigenen Captive-(Rück-)Versicherungsgesellschaft in der Regel nur bei einem gewissen Mindestgeschäftsvolumen verbunden mit einer längerfristigen Perspektive sinnvoll.

Nutzung einer bestehenden Infrastruktur (Rent-a-Captive, Protected Cell Company)

Alternativ bietet sich die Nutzung einer bestehenden Infrastruktur auf Basis einer entsprechenden vertraglichen Vereinbarung an, welche in der Regel mit einem geringeren Aufwand und höherer Flexibilität verbunden ist. Als Ausprägungen dieser Captive-Form sind die sogenannte „Rent-a-Captive“ sowie die Protected Cell Company zu nennen. Die „Rent-a-Captive“-Lösung ist vergleichbar mit einem Konto, das ein Versicherer für den Versicherungsnehmer führt und über das die Eigentragung des Versicherungsnehmers abgewickelt wird. Dem Konto werden die Anteile der vom Versicherer vereinbahrten Prämie gutgebracht, welche der vereinbarten Risikoeigentragung entsprechen. Zudem werden die auf

die auf dem Konto befindlichen Mittel erzielen Kapitalanlageerträge gutgeschrieben. Im Rahmen der Eigentragung anfallende Schäden sowie Gebühren für die Nutzung der Rent-a-Captive Lösung werden dem Konto belastet. Ein positiver Kontosaldo am Ende der Versicherungsperiode steht dem Versicherungsnehmer zu, ein negativer Saldo ist vom Versicherungsnehmer auszugleichen. In jüngster Zeit verliert das Rent-a-Captive Konzept nicht zuletzt aufgrund aufsichts- und steuerrechtlicher Entwicklungen zunehmend an Relevanz. Abb. 17.1 illustriert das Konzept (vgl. Wöhrmann und Bürer 2001, S. 16):

Eine Protected Cell Company ist von der Funktionsweise der Rent-a-Captive-Lösung grundsätzlich vergleichbar. Die Cells sind Bestandteil einer sogenannten Protected Cell Company (PCC), die sich zum Beispiel im Eigentum von großen Versicherungsmaklerunternehmen oder auch versicherungsunabhängigen Unternehmen befinden. Die PCC ist eine Rechtsperson, die zum Betreiben des Erst- bzw. Rückversicherungsgeschäfts lizenziert ist. Innerhalb dieser Gesellschaft besteht eine grundsätzlich unbeschränkt hohe Anzahl an Zellen (Cells). Diese Zellen verfügen nicht über eine eigene Rechtsperson, jedoch sind die Vermögengegenstände einer Zelle gegen Ansprüche anderer Zellen geschützt (daher der Begriff protected). Jede Zelle bildet quasi einen virtuellen Versicherer bzw. Rückversicherer innerhalb der PCC. Dieser virtuelle Versicherer kann zum Beispiel zum Zweck der Risikoeigentragung von einem Unternehmen „gemietet“ werden. Dies bedeutet, dass der PCC-Anbieter die gesamte Infrastruktur für die Zelle, zum Beispiel zur Abwicklung der entsprechenden Erst- oder Rückversicherungsverträgen oder der aufsichtsrechtlichen Anforderungen zur Verfügung stellt. Da der Anbieter nur die Infrastruktur stellt, jedoch keine Risiken aus der Geschäftstätigkeit des virtuellen Versicherers übernimmt, sind durch

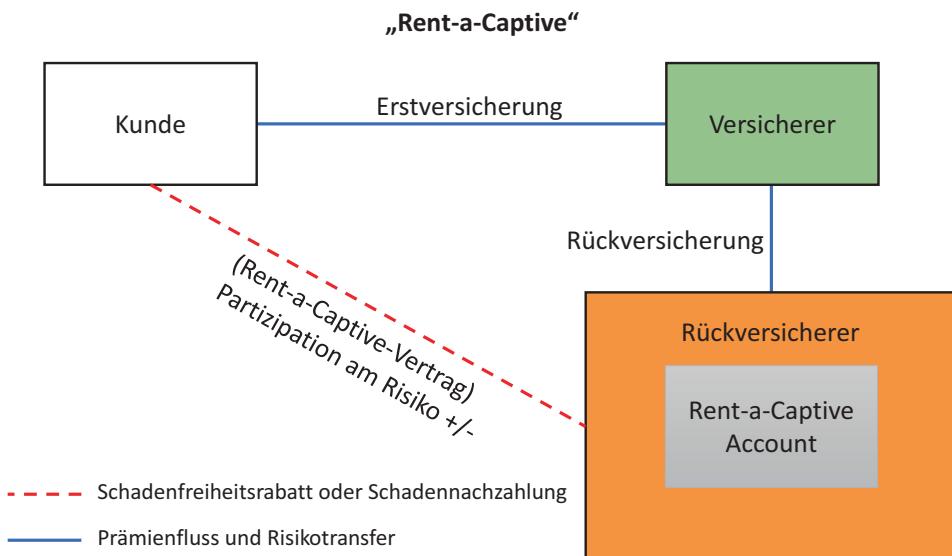


Abb. 17.1 Rent-a-Captive-Konzept. (Quelle: eigene Darstellung in Anlehnung an Wöhrmann und Bürer 2001, S. 16)

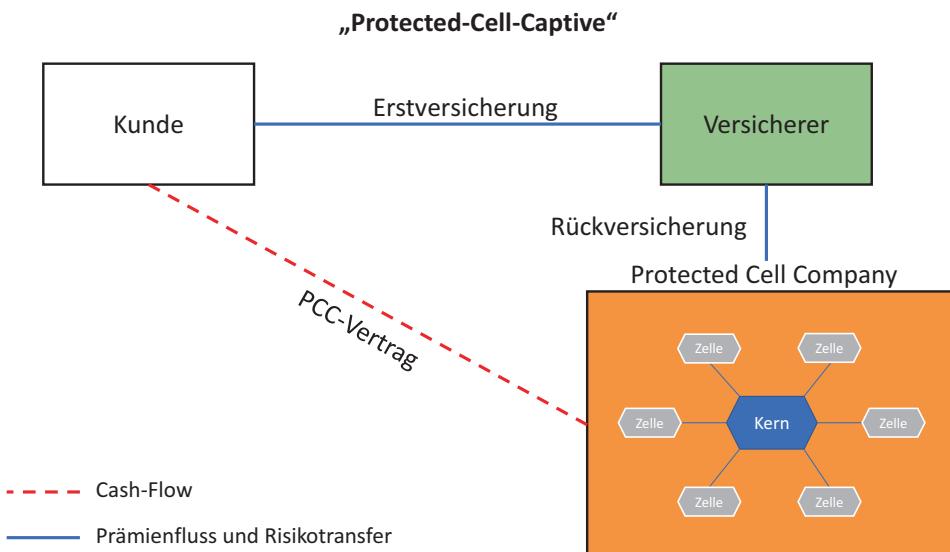


Abb. 17.2 Protected-Cell-Captive-Konzept. (Quelle: eigene Darstellung in Anlehnung an Wöhrmann und Bürer 2001, S. 16)

den Nutzer der Zelle entsprechende Sicherheiten zu stellen. Da die Infrastruktur von einer Vielzahl von Zellen genutzt werden kann, sind die Betriebskosten in der Regel vergleichsweise niedrig. Abb. 17.2 illustriert das Konzept.

17.4.2 Erstversicherung vs. Rückversicherung

Eine Captive kann als Erst- oder Rückversicherungsgesellschaft ausgestaltet werden.

Erstversicherung

Eine Erstversicherungscaptive ist wie ein Versicherungsunternehmen in der Lage, in verschiedenen Ländern, auf welche sich die Lizenz zum Betrieb des Versicherungsgeschäftes bezieht, Versicherungsverträge direkt mit dem Versicherungsnehmer, das heißt in der Regel der jeweiligen Tochtergesellschaft des Captive-Mutterunternehmens abzuschließen, Prämien zu erheben und Schäden zu regulieren. Aufgrund dieser Tatsache unterliegen Erstversicherungscaptives in der Regel höheren aufsichtsrechtlichen Anforderungen als Rückversicherungscaptives.

Eine in der EU domiziilierte Erstversicherungscaptive ist zum Beispiel in der Lage, auf Basis des Prinzips der Dienstleistungsfreiheit innerhalb der EU Direktgeschäft zu zeichnen (vgl. Fläming 2007, S. 57 f.). Damit wird kein vorzeichnender Versicherer (Fronter) benötigt und es entfallen Frontinggebühren und die Notwendigkeit, häufig von Fronter geforderte Sicherheitsleistungen in Form von Bankgarantien oder Bürgschaften zu stellen. Für

Länder außerhalb der EU besteht die Möglichkeit der Direktzeichnung in der Regel nicht. Sollen auch Risiken in Länder, die nicht von der Erstversicherungslizenz umfasst sind, Risiken gezeichnet werden, so ist dies nur auf dem Wege der Rückversicherung möglich. Erstversicherungscaptives betreiben daher in vielen Fällen nicht ausschließlich Erstversicherungsgeschäft, sondern auch aktives Rückversicherungsgeschäft. Die Zulässigkeit der Kombination ist vom jeweiligen Domizil der Captive abhängig. So ist zum Beispiel in Deutschland der Betrieb des aktiven Rückversicherungsgeschäfts nur in Sparten zulässig, in welchen auch Erstversicherungsgeschäft betrieben wird, in anderen Ländern ist der Anteil des Prämienvolumens aus aktiver Rückversicherung am Gesamtprämienvolumen der Captive begrenzt. Darüber hinaus ist in einigen Ländern die Kombination von Leben- und Nichtlebensversicherungsgeschäft in einer Erstversicherungsgesellschaft nicht zulässig.

Rückversicherung

Eine als Rückversicherungsgesellschaft lizenzierte Captive kann nicht in eine direkte Versicherungsvertragsbeziehung mit dem Versicherungsnehmer treten. Sie kann Risiken nur von einem vorzeichnenden Versicherer (Fronter) übernehmen. Der Fronter ist/sind in der Regel der führende bzw. die führenden Versicherer eines oder mehrerer internationaler Versicherungsprogramme des Captive-Mutterunternehmens. Dieser stellt die Policien für die jeweiligen Tochtergesellschaften aus, erhebt die Prämien und reguliert die Schäden. Prämien und Schäden werden durch den Fronter häufig zentral gepoolt und die Rückversicherungscaptive erhält in vertraglich vereinbarten Rhythmus Abrechnungen zu Prämien und Schäden für den von ihr übernommenen Risikoanteil. Ein Großteil der im Zusammenhang mit einem Versicherungsprogramm anfallenden Verwaltungstätigkeiten wird in dieser Konstellation durch den Fronter übernommen. Für diese Leistungen erhält er von der Captive ein Rückversicherungsprovision oder Fronting-Fee. Da der Fronter das Risiko trägt, dass die Captive möglicherweise nicht in der Lage ist, ihren Verpflichtungen aus dem Rückversicherungsvertrag nachzukommen (Gegenparteirisiko), werden in Abhängigkeit von Finanzkraft und ggf. Rating der Captive teilweise zusätzliche Sicherheiten zugunsten des Fronters gefordert.

Bei der Entscheidung bezüglich Erst- oder Rückversicherungscaptive sind folglich insbesondere die Belegenheit der Risiken, der unmittelbare Betriebsaufwand (Administration des Versicherungsprogramms, Erfüllung der aufsichtsrechtlichen Anforderungen) und das Zielgeschäftsmodell (Kombination von Leben- und Nichtlebensversicherungsgeschäft) relevante Kriterien. Während in der Vergangenheit die Eigentragung von betrieblichen Risiken im Vordergrund stand, rückt insbesondere für global tätige Unternehmen der Bereich der firmenfinanzierten Personenversicherungen immer stärker in den Fokus, da Gruppenleben-, -unfall-, -berufsunfähigkeits- und -krankenversicherungen, welche von Unternehmen als Teil des Vergütungspakets für ihre Mitarbeiter angeboten werden, vielfach signifikante Effizienz- und Transparenzpotenziale bieten.

17.4.3 Single Parent Captive vs. Multi Parent Captive

Eine Captive kann sich im Eigentum eines einzelnen (Single Parent) oder mehrerer Unternehmen befinden (Multi Parent).

Single Parent Captive

Eine Single Parent Captive ist ein Erst- oder Rückversicherungsunternehmen, welches sich im Eigentum eines einzelnen Unternehmens oder Konzerns befindet. Eine entsprechende Gesellschaft ist durch das Mutterunternehmen voll zu konsolidieren. Für das von der Captive gezeichnete Risiko können damit Ergebnisglättungseffekte, wie sie sich bei Transfer des Risikos auf einen Versicherer ergeben würden nur auf Ebene der versicherten Konzernchtergesellschaften, nicht jedoch auf Ebene des Mutterunternehmens erzielen lassen. Die überwiegende Anzahl von Captives weltweit sind in Form von Single Parent Captives vorzufinden (vgl. Fläming 2007, S. 60).

Multi Parent Captive

Sofern sich mehrere Unternehmen zusammenschließen, um eine Captive zu gründen und zu betreiben, wird dieser Verbund als Multi Parent Captive bezeichnet. Diese Form von Captives weist Ähnlichkeiten mit dem in Deutschland vorzufindenden Versicherungsverein auf Gegenseitigkeit (VVaG) auf. Die am häufigsten auftretenden Formen des Multi Parent Captives werden im weiteren Verlauf erklärt (vgl. Fläming 2007, S. 60).

Group-Captive

Wenn eine Gruppe von Unternehmen eine Group-Captive gründet und die Unternehmen Teilnehmer in gleichen Industrien sind, spricht man von Association- oder Industry-Captives. Die Captive-Betreiber statthen die Group-Captive mit dem notwendigen Gründungskapital aus. Im Vergleich zur Gründung eines Single Parent Captive ist der einzubringende Betrag pro Unternehmen geringer. Risiken und Prämien werden von den teilnehmenden Unternehmen in den Versicherungsbestand eingebbracht und anfallende Schadenzahlungen erfolgen aus dem gebildeten Prämienpool. Während viele Unternehmen in den USA in der harten Marktphase keine traditionellen Versicherungslösungen mehr am Markt einkaufen konnten, wurden die Group-Captives ins Leben gerufen. Ein Beispiel dafür ist OIL, eine Captive der petrochemischen Industrie in den USA. Ein wesentlicher Vorteil liegt zum einen im Risikoausgleich über die Zeit, zum anderen darin, dass Schadenzahlungen an die Teilnehmer gleichmäßiger über die Zeit verteilt anfallen, als dies für jeden Teilnehmer allein der Fall wäre. Das eingebrachte Kapital und die Prämien werden bei Verlusten als Deckung herangezogen (vgl. Fläming 2007, S. 60).

Risk Retention Group

Neben den Group-Captives sind Risk Retention Groups in den USA eine weitere verbreitete Spezialform von diesen. Risk Retention Groups sind von ihren Mitgliedern gegründete Haftpflichtversicherungsunternehmen, die mit Kapital ausgestattet werden und deren

firmeneigene Haftpflichtrisiken in ihr Versicherungsportfolio aufnehmen. Die Risiken, die Mitglieder in diese Form der Captives einbringen, stammen dabei aus gleichen oder zumindest ähnlichen Tätigkeitsbereichen, um ein möglichst homogenes Portfolio von Haftpflichtrisiken zu bilden. Bezogen auf die Haftung werden alle Mitglieder gesamtschuldnerisch gegenüber Ansprüchen von Dritten haften. Die Absicherung von Haftpflichtrisiken in dieser Form ist in den 80er Jahren des letzten Jahrhunderts entstanden, als sich viele US-amerikanische Versicherer aufgrund einer Krise des Versicherungsmarktes beziehungsweise des Haftpflichtversicherungsmarktes zurückgezogen haben. Durch die eingeschränkten Versicherungsmöglichkeiten im Jahre 1986 wurden den Risk Retention Groups erlaubt, neben der Absicherung von Produkthaftpflicht, auch die Absicherung von anderen Haftpflichtparten gestattet. Anfangs sollten die Klagewellen gegen Fabrikanten somit eine Absicherungsmöglichkeit gegeben werden. Mittlerweile gibt es Risk Retention Groups auch in anderen Industrien, wie zum Beispiel im Dienstleistungssektor und Gesundheitswesen. In den USA können Risk Retention Groups in allen anderen Bundesstaaten Geschäft zeichnen, wenn sie bereits in einem Bundesstaat eine Lizenz zum Versicherungsbetrieb besitzen (vgl. Fläming 2007, S. 60 f.).

17.4.4 Eigenrisikotragung (Pure Captive) vs. Drittgeschäft (Broad oder Open Market Captive)

Captive können mit der Zielsetzung gegründet und betrieben werden, ausschließlich unternehmenseigene Risiken zu versichern oder rückzuversichern (Pure Captive) oder auch fremde Risiken zu zeichnen (Broad oder Open Market Captive).

Pure Captive

Eine Pure Captive zeichnet ausschließlich Risiken, welche aus der betrieblichen Tätigkeit ihres Mutterunternehmens resultieren. Sie ist damit integraler Bestandteil und dient der Optimierung des Managements der versicherungsfähigen Risiken eines Unternehmens.

Da eine Pure Captive die Risiken eines einzigen Versicherungsnehmers zeichnet besteht kein Risikoportfolio vergleichbar einem am Markt tätigen Industriever sicherer, welcher eine Vielzahl von Risiken einer Vielzahl von Unternehmen bündelt und damit einen Risikoausgleich über das Kollektiv erreicht. Bei einer Pure Captive erfolgt der Risikoausgleich – in Abhängigkeit vom gezeichneten Geschäft – zu einem eher geringen Teil über den Portfolioeffekt und zum überwiegenden Teil über die Zeit. Pure Captives unterliegen in einigen Domizilen geringeren aufsichtsrechtlichen Anforderungen als Open Market Captives, da bei Nichterfüllbarkeit der versicherungsvertraglichen Verpflichtungen letztlich nur der frontende Versicherer bzw. das Mutterunternehmen finanziellen Schaden erleiden kann und daher der aufsichtsrechtliche Schutzfunktion eine geringere Bedeutung zukommt.

Broad oder Open Market Captive

Die Zeichnung unternehmensfremder Risiken über eine Captive erfolgt in der Regel aus Gewinnerzielungsabsicht und/oder steuerrechtlichen Überlegungen. Die Gewinnerwartung aus dem Betreiben des Versicherungsgeschäfts kann zum Beispiel auf spezifischer Expertise in einer Versicherungssparte aufgrund der Geschäftstätigkeit der Muttergesellschaft verbunden mit hoher Kosteneffizienz des Captive-Versicherers begründet sein. Ebenso ist der Verkauf von Versicherungen, welche an das Kernprodukt oder die Kerdienstleistung des Captive-Mutterunternehmens anschließen (zum Beispiel Garantieversicherung) zu beobachten.

Steuerrechtliche Erwägungen sind insofern relevant, als in einigen Ländern die Zeichnung eines Mindestanteils von Drittgeschäft seitens einer Captive Voraussetzung dafür ist, dass an die Captive gezahlte Prämien steuerlich als Betriebsaufwand geltend gemacht werden können (vgl. Fläming 2007, S. 63 f.).

17.5 Fazit

Mit der Einführung von Solvency II haben sich die aufsichtsrechtlichen Anforderungen an Captives mit Sitz in der EU insbesondere hinsichtlich Organisation des Geschäftsbetriebs, Dokumentation von Geschäftsprozessen und Verfahren sowie Berichterstattung an die Aufsichtsbehörden erheblich erhöht. Zudem sind Captives im Rahmen der OECD Initiative „Base Erosion and Profit Shifting“ (BEPS) als Instrumente identifiziert worden, welche zur Steuervermeidung eingesetzt werden können, so dass jeweils der Nachweis zu führen ist, dass dies nicht der Fall ist. Beide Entwicklungen tragen dazu bei, dass sich der Aufwand für das Betreiben einer Captive insbesondere sofern sie in der EU beheimatet ist, erhöht. Daraus folgt, dass das Geschäfts- bzw. Prämienvolumen, welches für den wirtschaftlichen Betrieb einer Captive erforderlich ist, ebenfalls gestiegen ist und sich damit der Kreis der Unternehmen, für welche eine Captive sinnvoll ist, tendenziell reduziert. Ein anderes Bild ergibt sich in den USA, wo Captives aufgrund der lokalen Rahmenbedingungen auch für kleinere Unternehmen mit geringerem Prämienvolumen weiterhin interessant sind. In Asien und Afrika ist bisher nur eine geringe Anzahl von Captives zu beobachten.

Unternehmensseitig wird die weitere Entwicklung hinsichtlich Captives – insbesondere, wenn es sich um eigene Tochtergesellschaften handelt – davon geprägt sein, welche Meinung hinsichtlich der Instrumente besteht, welche nicht unmittelbar dem Kerngeschäft dienen und mit einer gewissen Komplexität behaftet sind.

Auch die Entwicklung des Versicherungsmarktes hat einen Einfluss auf die Captive-Landschaft. In einem Verkäufermarkt, das heißt in Phasen, in denen Prämien und Deckungsumfang eher durch die Versicherer definiert werden, wird die Anzahl der Captive-Gründungen eher zunehmen, in einem Käufermarkt eher abnehmen.

Aufgrund der Vielzahl der Determinanten für die Entscheidung eine Captive zu gründen und zu betreiben – verbunden mit einer gewissen Dynamik ihrer Entwicklung – fällt es schwer einen generellen Trend auszumachen.

Für das Unternehmen, welches sich mit dem Gedanken trägt, eine Captive zu gründen, oder den Weiterbetrieb einer bestehenden Captive (inklusive einer möglichen Sitzverlegung) kritisch hinterfragt, gilt es, neben der Wirtschaftlichkeitsrechnung insbesondere die standortbezogenen Parameter aufsichtsrechtliches Umfeld und Anforderungen, steuerliche Bewertung, Reputation und Infrastruktur zu prüfen, wobei diese Parameter regelmäßig in Konkurrenz zueinander stehen.

Literatur

- Auras, R. (2017). Captives und Solvency II – wie passt dies zusammen? *Die Versicherungspraxis*, Ausgabe 11, S. 3–6.
- Captive Review. (2019). World Domicile Update 2019. *Captive Review*, Ausgabe Juni 2019.
- Erdmann, R. (2017). Evaluierung Einer Captive – Viel Aufwand Oder Echter Ertrag? *Die Versicherungspraxis*, Ausgabe 11, S. 13–14.
- Fläming, M. (2007). Alternativer Risiko Transfer – eine volkswirtschaftliche Betrachtung, Universität Bamberg. <https://opus4.kobv.de/opus4-bamberg/frontdoor/index/index/docId/151>. Zugriffen am 29.03.2019.
- Grund, F. (2017). Die Herausforderungen der proportionalen Aufsicht über Captives. *Die Versicherungspraxis*, Ausgabe 11, S. 7–8.
- Ilić, I. (2012). Traditionelle Rückversicherung im Vergleich mit modernen und alternativen Formen des Risikotransfers, Universität Wien. <https://core.ac.uk/download/pdf/16427276.pdf>. Zugriffen am 29.03.2019.
- International Risk Management Institute, Inc. (2019). The early days of captives (through 1984). <https://www.captive.com/resources/captive-insurance-history/before-1985>. Zugriffen am 17.04.2019.
- Palmerberger, H. (2016). Captives in Selbsttragungsmodellen Vor- und Nachteile. *Die Versicherungspraxis*, Ausgabe 12, S. 6–7.
- Rohlf, T. (2018). *Risikomanagement im Versicherungsunternehmen* (2. Aufl.). Karlsruhe: Versicherungswirtschaft.
- Telefónica Insurance S. A. (2017). Ihre beste Versicherung. <https://www.telefonicainsurance.de>. Zugriffen am 18.04.2019.
- Willis Tower Watson. (2016). Base erosion & profit shifting (BEPS) analysis for captives – Meeting the OECD's BEPS action plan. [https://www.willis.com/documents/publications/services/captives/Willis%20Towers%20Watson%20BEPS%20analysis%20for%20captives%20\(1\).pdf](https://www.willis.com/documents/publications/services/captives/Willis%20Towers%20Watson%20BEPS%20analysis%20for%20captives%20(1).pdf). Zugriffen am 29.04.2019.
- Wöhrmann, P., & Bürer, C. (2001). Procted Cell Captives: Auch für die Schweiz geeignet?. *Schweizer Versicherung*, Ausgabe 7, S. 16.

Holger Kraus studierte Betriebswirtschaftslehre mit Schwerpunkt Risikomanagement und Versicherung an der Universität St. Gallen (HSG). Nach Abschluss des Studiums war er mehrere Jahre für Aon in der Beratung von Großunternehmen zu alternativen Risikofinanzierungslösungen und Captives tätig. Seit 2009 ist er im Bereich Versicherungen der Siemens AG für Risikofinanzierung und Strategie verantwortlich und zudem Vorsitzender des Vorstands der RISICOM Rückversicherung AG, dem konzerneneigenen Rückversicherer der Siemens AG. Darüber hinaus leitet er den Captive-Ausschuss des Verbands der versicherungsnehmenden Wirtschaft (GVNW).

Julian Alexander Robles Häusser studierte Versicherungswesen mit den Schwerpunkten HUKR (Haftpflicht-, Unfall-, Kraftfahrt- und Rechtsschutzversicherung), Sachversicherung und Personal am Institut für Versicherungswesen der Technischen Hochschule Köln. Im Anschluss absolvierte er dort auch das Masterstudium Risk & Insurance. Vor dem Studium hat er eine Ausbildung zum Kaufmann für Versicherungen und Finanzen gemacht. Aktuell arbeitet er bei der ROLAND Rechtsschutz-Versicherungs-AG in Köln als Referent Underwriting.



Rolle des Rückversicherers in der Industriever sicherung

18

Angelika Trotta und Jan Fischer

Zusammenfassung

Der folgende Beitrag gibt einen Einblick in die Rolle des Rückversicherers in der Industriever sicherung. Zu Beginn wird ein Überblick über den aktuellen traditionellen Rückversicherungsmarkt gegeben. Im darauffolgenden Abschnitt werden die Grundlagen der Rückversicherung erläutert. Des Weiteren werden die verschiedenen Rückversicherungsformen und Vertragsarten, inklusive wichtiger vertraglicher Gestaltungsaspekte, genauer beschrieben. Diese umfassen die obligatorischen und fakultativen Vertragsarten sowie proportionale und nicht-proportionale Vertragsformen und deren Wirkungsweise innerhalb eines Rückversicherungsprogrammes.

Danach werden die Rückversicherungssparten, deren besonderen Gefahren und Rückversicherungsdeckungskonzepte für Industrierisiken dargestellt. Im Anschluss werden die allgemeinen Ausschlüsse der Rückversicherung beschrieben, um im nächsten Schritt die Grenzen der Rückversicherung aufzuzeigen. Im letzten Abschnitt wird der besondere Mehrwert der Rückversicherung für Industrikunden herausgestellt.

Ziel dieses Beitrages ist es, die traditionelle Rückversicherung in ihren Grundlagen zu erklären und dem Leser einen Einblick in die Nutzung von Rückversicherung zum Transfer von industriellen Risiken zu gewähren. Indem der Mehrwert der Risikotragung auf globaler Rückversicherungsebene für Industrikunden herausgearbeitet wird, wird gezeigt, dass Rückversicherung mehr ist als die Versicherung von Versicherungsunternehmen.

A. Trotta (✉)

General Reinsurance AG, Köln, Deutschland

E-Mail: angelika.trotta@genre.com

J. Fischer

TH Köln, Institut für Versicherungswesen, Köln, Deutschland

E-Mail: janfischer1990@gmail.com

18.1 Einleitung

18.1.1 Rückversicherung – mehr als die Versicherung von Versicherungsunternehmen?

Die traditionelle Rückversicherung ist ein wichtiger Bestandteil der Wertschöpfungskette der Versicherungsindustrie. Weltweit trägt die Rückversicherungsindustrie zur Stabilität der Wirtschaft bei. Ziel eines Erstversicherungsunternehmens ist es durch den Transfer von (Teil-)Risiken das versicherungstechnische Risiko effizienter zu steuern und, damit verbunden, den Ausgleich im Kollektiv und in der Zeit zu optimieren. Zufalls-, Änderungs- und Irrtumsrisiken können durch geeignete Rückversicherungslösungen vermindert werden. Aus Sicht der Risikolage des Erstversicherungsunternehmens kann Rückversicherung auch als ein Instrument zur Optimierung von Kapitalstrukturen herangezogen werden. Im klassischen Sinne der Rückversicherung schützt sich der Erstversicherer vor Groß- und Kumulschäden und deckt somit Spaltenrisiken ab. Beispiele hierfür sind Schäden verursacht durch Stürme, Erdbeben oder Flut. Des Weiteren bietet der Rückversicherer Unterstützung bei der Zeichnung von weltweiten Risiken im Rahmen von Services und internationalem Knowhow an.

In diesem Kapitel soll deutlich werden, dass Rückversicherung mehr ist als nur die Versicherung eines Versicherungsunternehmens. Gerade aus Perspektive der Industrie bietet die Rückversicherung einen signifikanten Mehrwert. Durch die Erweiterung der Bruttozeichnungskapazitäten (Zeichnungskapazität vor Abzug von Rückversicherung) und der Teilung des versicherungstechnischen Risikos wird ein Erstversicherer dazu befähigt, gerade besonders große und/oder besonders exponierte Risiken eines Industrieunternehmens in seinen Bestand aufnehmen zu können. Der Rückversicherer wiederum ist in der Lage, globale Spaltenrisiken durch seine Kapitalstärke in einem weltweiten Kollektiv auszugleichen.

Im Folgenden wird die Rolle des Rückversicherers im Industriegeschäft genauer beleuchtet. Zunächst werden die Grundlagen der obligatorischen und fakultativen Rückversicherung und deren Vertragsformen beschrieben. Im darauffolgenden Abschnitt wird die Rückversicherung in Bezug auf die Risiken des internationalen Industriegeschäfts aufgezeigt. Neben den klassischen in Rückdeckung gegebenen Gefahren aus den verschiedenen Versicherungssparten wird ein besonderer Fokus auf die Bedeutung, auf den Mehrwert, aber auch auf die Grenzen der Rückversicherung im Industriegeschäft gelegt.

18.1.2 Ein Überblick des nationalen und internationalen Rückversicheremarktes

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) beaufsichtigt in Deutschland um die 40 in- und ausländische Rückversicherungsunternehmen mit Bruttobeiträgen in der Höhe von rund 59,7 Milliarden Euro (Stand 2017, vg. BaFin 2018, S. 7 f.). Zu den

größten Rückversicherungsunternehmen zählen Munich Re, Swiss Re, Gen Re (Berkshire Hathaway) und Hannover Re (vgl. Sheehan 2018, S. 1). Bedeutende Rückversicherungsmakler sind unter anderem AON, Willis Re und Guy Carpenter. International stellt der Versicherungsmakler Lloyds of London unter anderem Rückversicherungskapazitäten für besonders exponierte Risiken mit sehr hohen Versicherungssummen zur Verfügung. Beispielsweise wird über Lloyds of London die von üblichen Rückversicherungsverträgen ausgeschlossene Beförderung von Satelliten in die Erdumlaufbahn (rück-)versichert. Zu den teuersten getragenen Schäden der Rückversicherungsindustrie zählen Hurrikan Katrina im Jahre 2005, das Erdbeben/der Tsunami in Japan in 2011 und Hurrikan Maria in 2017. Der Terroranschlag vom 11. September 2001 war der bislang teuerste von Menschen verursachte Großschaden für die Rückversicherer (vgl. Bevere et al. 2018, S. 48). Im Durchschnitt der letzten fünf Jahre zahlten Rückversicherer jährlich Schäden im Wert von mehr als 110 Milliarden US-Dollar aus (vgl. McKinsey & Company 2017, S. 3).

Typischerweise durchläuft der globale Rückversicherungsmarkt Zyklen. In Weichmarktphasen steht mehr Kapazität als benötigt zur Verfügung, was eine Preisreduzierung zur Folge haben kann. Im Gegensatz dazu können sich in Hartmarktphasen die Kapazitäten der Rückversicherer reduzieren und Preise entsprechend ansteigen. In der Vergangenheit folgte einem besonders teuren Schadeneignis oder Schadenjahr häufig ein verhärteter Markt. Darüber hinaus wird der traditionelle Rückversicherungsmarkt verstärkt durch alternative Formen von Rückversicherungskapazitäten beeinflusst, welche im nächsten Kapitel weiter beschrieben werden sollen. Das globale Rückversicherungskapital betrug in den letzten fünf Jahren ca. 500 Milliarden US-Dollar, wobei alternatives Kapital rund ein Sechstel hiervon ausmachte (vgl. AON 2019, S. 3).

18.2 Grundlagen der Rückversicherung

18.2.1 Arten und Formen der Rückversicherung

Die traditionelle Rückversicherung lässt sich in die Bereiche obligatorische und fakultative Rückversicherung unterteilen. Bei der obligatorischen Rückversicherung, auch Vertragsrückversicherung genannt, einigen sich Erst- und Rückversicherer darauf, dass alle Risiken, welche sich im vereinbarten Rahmen des Rückversicherungsvertrages befinden, ohne weitere Prüfung des Rückversicherers in Rückdeckung genommen werden. Hierbei handelt es sich meistens um eine größere Anzahl Risiken einer Versicherungssparte, um ein sogenanntes Portefeuille. Im Gegensatz dazu werden in der fakultativen Rückversicherung nur einzelne (Teil-)Risiken-/Policen an den Rückversicherer abgegeben. Man spricht hierbei von einer Zession, also der Abgabe von (Teil-)Risiken des Erstversicherers an den Rückversicherer. Jedes Risiko unterliegt vor Abschluss eines fakultativen Rückversicherungsvertrages einer genauen Prüfung. Im Unterschied zur obligatorischen Rückversicherung haben Erst- und Rückversicherer die Wahl, ob das einzelne Risiko angenommen oder abgelehnt werden soll (vgl. Liebwein 2018, S. 61 f.).

Neben der Art wird auch zwischen der Form der Rückversicherung unterschieden. Bei den Formen der Rückversicherung unterteilt man in proportionale und nicht-proportionale Zessionen. Im Wesentlichen unterscheiden sich diese beiden Grundformen darin, ob die Alimentierung basierend auf der Versicherungssumme oder basierend auf der Schadenhöhe erfolgt.

18.2.1.1 Proportionale Rückversicherung

Bei der proportionalen Rückversicherung werden Prämien und Schäden anhand von Haftungsverhältnissen zwischen Erst- und Rückversicherer proportional aufgeteilt. Die Aufteilung erfolgt auf Basis der Gesamtversicherungssumme oder des Probable Maximum Loss (PML). Da der Rückversicherer einen bestimmten Prozentsatz aller der Haftung entsprechenden Schäden übernimmt, kann hierbei ein Jahreslimit für übernommene Schäden vereinbart werden, um dadurch den Gesamtschaden des Rückversicherers zu begrenzen.

Zusätzlich erhält der Erstversicherer eine Provision zur Deckung von zum Beispiel Administrationskosten. Diese Provision ist verhandelbar und unter anderem auch abhängig von der Qualität der unterliegenden Risiken oder des einzelnen Risikos. Daher kann die Provision auch als ein Preisindikator für proportionale Rückversicherungsverträge verstanden werden. Sie wird üblicherweise als Prozentsatz auf den zedierten Anteil an den Rückversicherer ausgedrückt (vgl. Liebwein 2018, S. 69 f.).

Quotenrückversicherung

Bei der Quotenrückversicherung werden Prämien und Schäden anhand einer festen Quote zwischen beiden Vertragsparteien aufgeteilt. Diese Quote wird vor Vertragsabschluss verhandelt. Beträgt sie zum Beispiel 50 Prozent, so fließt die Hälfte aller eingenommenen Prämien an den Rückversicherer. Im Schadenfall trägt der Rückversicherer im Gegenzug die Hälfte des Schadensaufkommens. Die Quotenrückversicherung eignet sich sowohl für fakultative als auch für obligatorische Rückversicherungsvereinbarungen.

Ein Vorteil der Quotenrückversicherung ist die Verringerung der absoluten Haftung des Erstversicherers. Daher kann diese Vertragsform zur Reduzierung des benötigten Solvenzkapitals beitragen. Man spricht in diesem Zusammenhang auch von Rückversicherung als Eigenkapitalsubstitut. Des Weiteren kann eine Quotenrückversicherung zur Finanzierung und zum Aufbau von Neugeschäft genutzt werden, um den anfänglich hohen Kosten, generiert durch Wachstum, entgegenzuwirken. Nachteilig ist, dass die Quotenrückversicherung nur bedingt Schutz gegen Groß- und Kumulschäden bietet, da diese nur anteilig übernommen werden. Eine Homogenisierung der Exponierungen (Versicherungssummen oder Schäden) innerhalb eines Portefeuilles findet also nicht statt. Unter der Voraussetzung, dass die Provision der Quotenabgabe den Originalkosten entspricht, bleiben Brutto- und Netto-Schadenquote bei dieser Form der Rückversicherung gleich (vgl. Gerathewohl 1976a, S. 102 f.; vgl. Abb. 18.1).

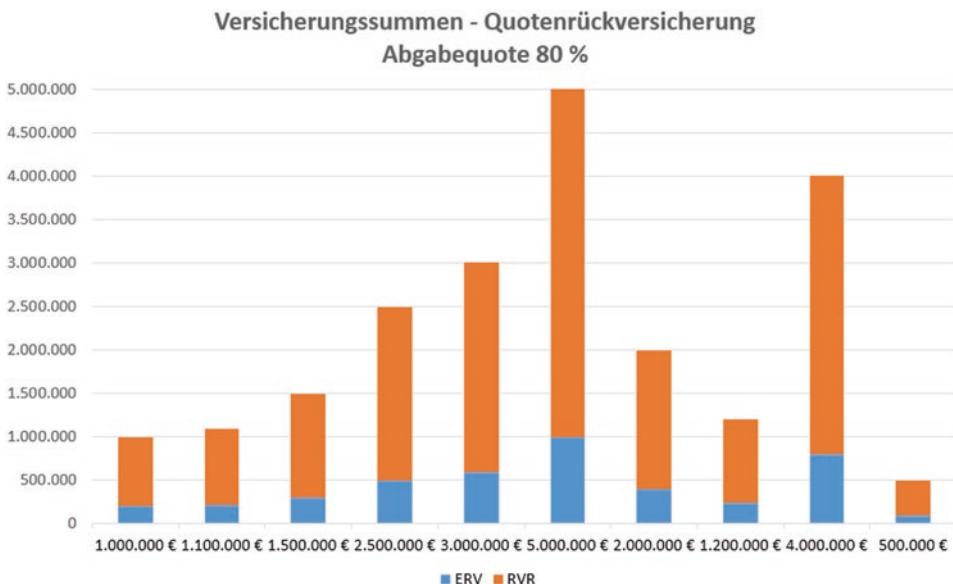


Abb. 18.1 Beispiel: Wirkungsweise Quotenrückversicherung. (Quelle: eigene Darstellung)

Summenexzedent

Eine weitere Form der proportionalen und obligatorischen Rückversicherung ist der sogenannte Summenexzedent. Auch bei dieser Vertragsform werden Prämien und Schäden proportional zwischen Erst- und Rückversicherer aufgeteilt. Jedoch erfolgt die Aufteilung im Verhältnis vom Selbstbehalt des Erstversicherers zum übernommenen Anteil der Versicherungssumme oder des PML. Der Rückversicherer stellt hierbei Kapazitäten in der Höhe eines Vielfachens des Selbstbehaltes des Erstversicherers zur Verfügung, die sogenannten Maxima. Der Selbstbehalt wird als Maximum bezeichnet.

Wird beispielsweise vereinbart, dass der Selbstbehalt des Erstversicherers 100.000 Euro beträgt und der Rückversicherer eine Kapazität von vier Maxima bereitstellt, dann teilen sich Prämien und Schäden für ein Risiko mit einer Versicherungssumme von 500.000 Euro in einem Verhältnis eins zu fünf auf. Risiken mit Versicherungssummen, welche den Selbstbehalt von 100.000 Euro übersteigen, werden anteilig vom Rückversicherer getragen. Übersteigt die Versicherungssumme jedoch 500.000 Euro, dann fällt der überschreitende Anteil des Risikos wieder zu Lasten des Erstversicherers. Maximal stellt der Rückversicherer also eine Haftstrecke von 400.000 Euro zur Verfügung. Risiken mit Versicherungssummen unter 100.000 Euro erhalten keine Entlastung durch diese Rückversicherung.

Insgesamt wird durch den Summenexzedenten die Bruttozeichnungskapazität des Erstversicherers erhöht. Spitzenrisiken eines Portefeuilles werden „abgeschnitten“, was eine Homogenisierung des Bestandes bewirkt. Jedoch trägt der Erstversicherer in jedem Fall einen Selbstbehalt an allen Risiken. Bei einer Kumulierung von Schäden, ausgelöst durch

ein Ereignis, führt dies zu einer hohen Schadenbelastung für den abgebenden Erstversicherer, den Zedenten (vgl. Gerathewohl 1976a, S. 71 f.; vgl. Abb. 18.2).

18.2.1.2 Nicht-proportionale Rückversicherung

In der nicht-proportionalen Rückversicherung werden Schäden ab Überschreiten der so-nannten Priorität, dem Beginn der Haftstrecke des Rückversicherers, bis zum sogenannten Plafond, der Summe aus Haftstrecke und Priorität, vom Rückversicherer getragen. Vor Abschluss des Rückversicherungsvertrages wird ein an den Rückversicherer zu zahlender Rückversicherungspreis bestimmt. Die originale Versicherungsprämie wird nicht in einem Verhältnis zwischen Erst- und Rückversicherer geteilt. Die Preisfindung, welche auch als Quotierung bezeichnet wird, basiert üblicherweise auf Schadensimulationen oder statistischen Verfahren, überwiegend durchgeführt durch Rückversicherer und Rückversicherungsmakler. Wichtige Preisfaktoren sind die Schadenhistorie, die erwartete Entwicklung des Portefeuilles, die Position des betreffenden Deckungsabschnitts und damit einhergehende Schadenverteilungskurven (zur Einschätzung der Schadenhöhenverteilung), die Marktphase oder die Einordnung der Rückversicherung innerhalb eines Rückversicherungsprogrammes (vgl. Liebwein 2018, S. 181 f.).

Eine der häufigsten nicht-proportionalen Vertragsformen ist der Schadenexzedent. Alle Schäden, welche die Priorität übersteigen, werden dabei bis zum Plafond vom Rückversicherer getragen. Häufig wird die Haftstrecke in Deckungsabschnitte, auch Layer genannt, unterteilt. Die Anzahl der Layer ist abhängig von der Höhe der gesamten Haftstrecke, sie können aber beliebig geschnitten werden. In der Regel sind niedriggelegene Layer teurer als höhergelegene Layer, da die Schadeneintrittswahrscheinlichkeit im Bereich kleiner bis

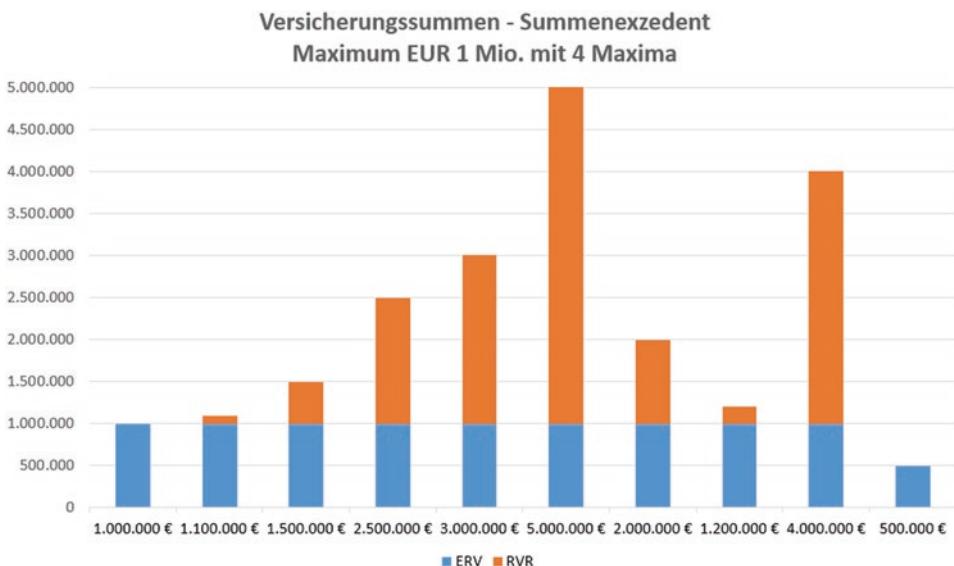


Abb. 18.2 Beispiel: Wirkungsweise Summenexzedent. (Quelle: eigene Darstellung)

mittlerer Schäden oberhalb der Priorität größer ist als bei Schäden, welche die gesamte Haftstrecke beanspruchen. Des Weiteren werden in der Praxis Haftstrecken oft mehrmals pro Jahr bereitgestellt. Wurde die erste Haftstrecke durch einen Schaden aufgebraucht, bietet der Rückversicherer eine oder mehrere Wiederauffüllungen an und stellt damit eine zusätzliche Haftstrecke zur Verfügung. Die Gestaltung der Wiederauffüllung kann variieren. Der Rückversicherungseinkäufer muss entscheiden, ob Wiederauffüllungen entweder pro rata capita (das heißt Zahlung entsprechend der verbrauchten Haftstrecke) oder pro rata temporis (das heißt Zahlung entsprechend von Zeitabschnitten) zu bezahlen sind oder ob hinzukommende Wiederauffüllungen vor Vertragsbeginn bezahlt oder unbezahlt vereinbart werden (vgl. Schwepcke 2004, S. 338 f.). Die Entscheidung, wie eine Wiederauffüllung gestaltet werden soll, ist abhängig von der Einschätzung der zukünftig anfallenden Schäden des Folgejahres. Wird beispielsweise nur ein Schaden erwartet, ist eine bezahlte Wiederauffüllung zu bevorzugen. Übersteigt ein definierter Schaden den Plafond der Deckung, trägt der Erstversicherer den überschreitenden Teil selbst. Somit können Schäden oberhalb des Plafonds als zusätzlicher Selbstbehalt für den Erstversicherers gesehen werden.

Eine weitere Unterteilung innerhalb der Schadenexzedenten der obligatorischen Rückversicherung ergibt sich in der Deckung pro Einzelschaden oder pro Ereignis.

Einzelschadenexzedent

Bei einem Einzelschadenexzedenten werden Schäden eines einzelnen Risikos vom Rückversicherer ab der Priorität getragen. Diese Vertragsform wird auch als Schadenexzedent pro Risiko bezeichnet und ist bei heterogenen Portefeuilles mit großen Risiken, also mit hohen Versicherungssummen/PML, vorteilhaft und üblich.

Einzelschadenexcedenten schützen vor Großschäden, zum Beispiel ausgelöst durch ein Feuer. Innerhalb eines Portefeuilles trägt der Einzelschadenexzedent zur Homogenisierung der Schadenzahlungen des Erstversicherers bei (vgl. Gerathewohl 1976a, S. 86 f.; vgl. Abb. 18.3).

Kumulschadenexzedent

Der Kumulschadenexzedent, auch Schadenexzedent pro Ereignis genannt, bietet Rückversicherungsschutz gegen Schadenereignisse, die eine Vielzahl von Risiken betreffen. Risikobspiele hierfür sind Stürme, Erdbeben oder Überschwemmungen, welche in den folgenden Abschnitten genauer beschrieben werden. Diese Ereignisse verursachen meist kleine bis mittlere Schadenhöhen, welche sich im Selbstbehalt des Erstversicherers, nach Abzug anderer vorangegangener Rückversicherungsformen, befinden. Im Gegensatz zum Einzelschadenexzedenten wird hier vereinbart, dass die Summe aller Schäden innerhalb des Selbstbehaltes vom Rückversicherer ab Beginn der Priorität bis zur Ausschöpfung der Haftstrecke getragen wird. Ereignisse und deren Gefahren werden innerhalb des Rückversicherungsvertrages genau definiert und geographisch und/oder zeitlich begrenzt (vgl. Liebwein 2018, S. 190 f.; vgl. Abb. 18.4).

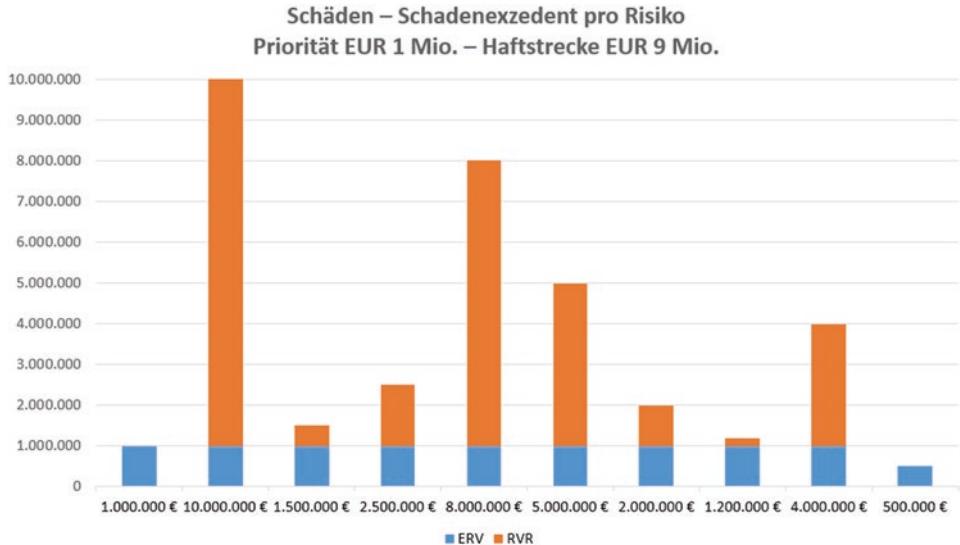


Abb. 18.3 Beispiel: Wirkungsweise Schadenexzedent pro Risiko. (Quelle: eigene Darstellung)

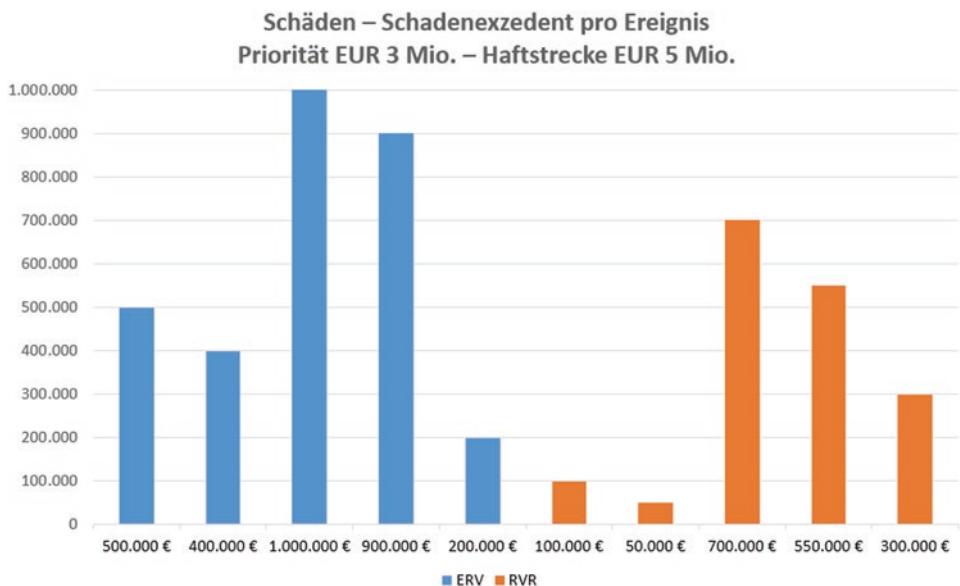


Abb. 18.4 Beispiel: Wirkungsweise Schadenexzedent pro Ereignis. (Quelle: eigene Darstellung)

Jahresüberschadenexzedent bzw. Stop Loss

Der Jahresüberschadenexzedentenrückversicherungsvertrag (kurz Stop Loss) aggregiert alle Schäden im Selbstbehalt des Erstversicherers innerhalb eines Jahres. Übersteigt die Summe der Schäden den Selbstbehalt des Erstversicherers, trägt der Rückversicherer alle

weiteren Schäden bis zu einem vereinbarten Limit. Die Priorität wird in dieser Rückversicherungsform oft als eine zu überschreitende Schadenquote ausgedrückt. Typischerweise ist der Selbstbehalt des Erstversicherers bei dieser Vertragsform hoch. Der Stop Loss unterscheidet sich auch darin, dass in der Praxis nur eine Haftstrecke ohne Wiederauffüllung angeboten wird. Außerdem folgt der Stop Loss meistens anderen Rückversicherungsformen, da der Rückversicherer auf alleiniger Basis eines Stop Loss eine sehr hohe Schadenlast haben würde. Dies würde sich wiederum auf den Preis der Rückversicherung negativ auswirken. Der Stop Loss deckt alle versicherungstechnischen Risiken ab und wird als bilanzschützend bezeichnet (vgl. Liebwein 2018, S. 201 f.; vgl. Abb. 18.5).

18.2.1.3 Fakultative Rückversicherung

Wie eingangs erwähnt wird in der fakultativen Rückversicherung nur eine einzelne Versicherungspolice oder ein Risikoausschnitt an den Rückversicherer zediert. Der Rückversicherer hat die Wahl, ob und in welcher Höhe er sich am Risiko beteiligen möchte. Dem Erstversicherer stehen jedoch mehrere Rückversicherer zur Auswahl, um das Risiko an den Rückversicherungsmarkt zu transferieren. Auch bei fakultativen Rückversicherungsverträgen wird zwischen proportionalen und nicht-proportionalen Vertragsformen unterschieden. Es kann eine proportionale Abgabekurve, welche Originalprämie und Schäden prozentual aufteilt, oder ein Schadenexzedent, welcher Schäden ab der Priorität deckt, vertraglich vereinbart werden. Die Unterscheidung zwischen Quotenrückversicherung und Summenexzedent oder Schadenexzedent pro Risiko und pro Ereignis findet in der

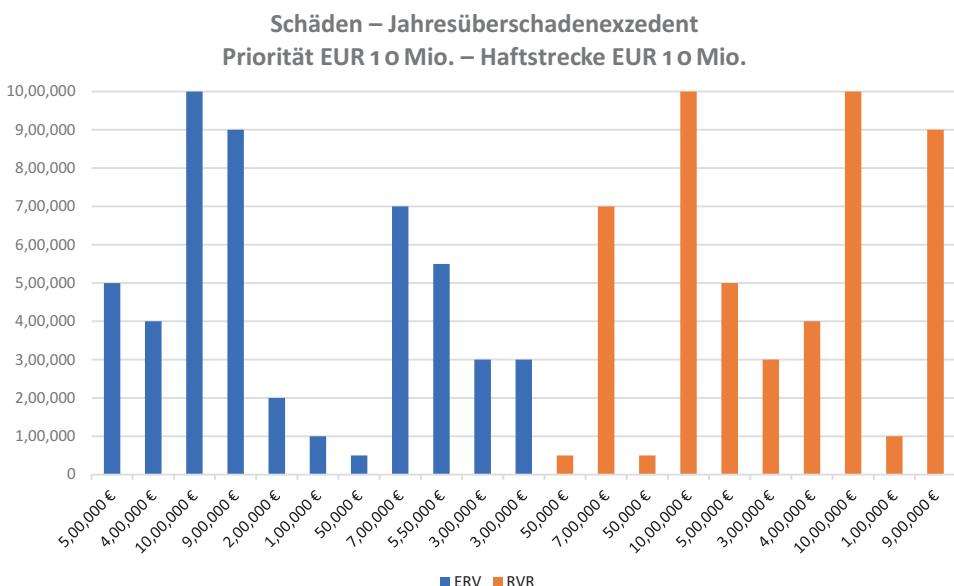


Abb. 18.5 Beispiel: Wirkungsweise Jahresüberschadenexzedent. (Quelle: eigene Darstellung)

fakultativen Rückversicherung hingegen keine Anwendung, da es sich hier eben nur um ein einzelnes Risiko handelt (vgl. Liebwein 2018, S. 61 f.).

Nun stellt sich die Frage, warum einzelne Risiken fakultativ rückversichert werden sollen. Der klassische Einsatz für die fakultative Rückversicherung ist die Erhöhung der Zeichnungskapazität für ausgewöhnlich große Risiken, welche besonders hohe Kapazitäten beanspruchen und damit über die obligatorisch vereinbarte Kapazität hinausgehen. Der Nutzen des fakultativen Rückversicherungsproduktes liegt aber auch darin, dass hiermit außergewöhnliche Risiken transferiert werden können. Diese befinden sich möglicherweise außerhalb der Rahmenbedingungen eines obligatorischen Rückversicherungsvertrages, wie zum Beispiel bei einem Risiko, welches sich außerhalb der vereinbarten geografischen Begrenzung des Vertrages befindet. Ziel hierbei ist eine weitere Homogenisierung des Portefeuilles. Mögliche Deckungslücken in der Rückversicherung sollen geschlossen werden. Außerdem werden fakultative Rückversicherungsverträge bei schweren Risiken vorweg abgeschlossen, um zum Schutz des Rückversicherungsvertrages eine Deckung von zum Beispiel Industrierisiken zu ermöglichen und gleichzeitig dem individuellen Risikoappetit zur Portefeuille-Steuerung gerecht werden zu können. Der Erstversicherer möchte sich in erster Linie gegen zusätzliche Großschäden aus heterogenem Geschäft schützen. Außerdem können über fakultative Rückversicherung bei einem Erstversicherer unerwünschte Betriebsarten und Gefahren rückversichert werden. Dies dient zum einen der Optimierung der Zeichnungspolitik, zum anderen trägt es auch zur Verbesserung der Wettbewerbsfähigkeit des Erstversicherers bei. Denn eine fakultative Abgabe kann den Erstversicherer in die Lage versetzen, den Versicherungsschutz besser auf die Kundenwünsche abzustimmen und anzubieten. In diesem Fall wird eine fakultative Ausschnitts- oder Gefahrenrückversicherung verwendet. Die fakultative Rückversicherung findet auch in neuen Geschäftsbereichen oder bei dem Versicherer fremden Versicherungssparten Anwendung. Durch die maßgeschneiderte fakultative Rückversicherung ist der Erstversicherer in der Lage, dem Kunden Deckung für außergewöhnliche Risiken anzubieten. Der Versicherer kann so vollumfänglichen Versicherungsschutz anbieten (vgl. Schwepcke 2004, S. 124 f.).

Nachteilig für Erst- und Rückversicherer ist der erhöhte Aufwand im Underwriting (Bewertung und Preis- und Kapazitätsfestsetzung von Risiken) und bei der Administration von fakultativen Einzelabgaben. Für jedes Risiko wird ein separater Rückversicherungsvertrag abgeschlossen. Vor Vertragsabschluss muss jedes Risiko durch den Rückversicherer geprüft, quotiert und akzeptiert werden. Der Erstversicherer muss das Risiko am Rückversicherungsmarkt anbieten und die ihm zur Verfügung stehenden Informationen weitergeben.

Besonders in der Industriever sicherung spielen solche außergewöhnlichen Risiken eine große Rolle, weshalb die fakultative Rückversicherung ein entscheidendes Instrument zur Absicherung aller versicherbaren Risiken eines Industrikunden darstellt.

18.2.1.4 Weitere Rückversicherungsvertragsbestandteile

Ein weiterer wichtiger Aspekt der Rückversicherung ist die Haftungsgrundlage des Rückversicherers. Hier ist zunächst zwischen Long-Tail- und Short-Tail-Geschäft zu unterscheiden. Als Long-Tail-Geschäft werden Versicherungssparten mit langen Schadenabwicklungs dauern bezeichnet. Im Gegensatz dazu ist die Abwicklungs dauer von Short-Tail-Geschäft eher kurz. Bei der Rückversicherung von Long-Tail-Geschäft wird großer Wert auf die Bonität des Rückversicherers gelegt, um sicherzustellen, dass mögliche Verpflichtungen aus Rückversicherungsverträgen in zukünftigen Jahren noch erfüllt werden können. Auch die Wahl der Basis des Beginns der Risikotragung durch den Rückversicherer spielt hierbei eine zentrale Rolle. Der Erstversicherer muss entscheiden, ob er den Rückversicherungsvertrag auf Zeichnungsjahrbasis oder auf Anfalljahrbasis abschließt. Bei einer Zeichnungsjahrbasis übernimmt der Rückversicherer Deckung für alle Risiken, welche in diesem Jahr in den Bestand aufgenommen wurden. Bei einer Anfalljahrbasis werden alle Schäden des rückversicherten Jahres, entsprechend der Vereinbarungen, an den Rückversicherer zediert (vgl. Liebwein 2018, S. 129 f.).

18.2.2 Rückversicherungsprogramme

Erstversicherungsunternehmen schützen sich mit einer Kombination aus verschiedenen Rückversicherungsvertragsarten und Formen. Dies soll im Folgenden am Beispiel eines Rückversicherungsprogrammes für ein heterogenes Sachversicherungspor tefeuille erklärt werden. Im Bereich der obligatorischen Rückversicherung wird zunächst eine Quoten rückversicherung vereinbart. Dies erhöht zum einen die Bruttozeichnungskapazität, reduziert aber andererseits anteilig die Schadenlast des Erstversicherers. Der Nettoselbstbehalt des Versicherungsunternehmens kann im nächsten Schritt durch nicht-proportionale obligatorische Rückversicherung geschützt werden. Hier werden meist mehrere Verträge, in Form von Layern, abgeschlossen. Der Erstversicherer möchte sich mit dem Einkauf eines oder mehrerer Einzelschadenexzedenten auf seinen Eigenbehalt unter der Quote gegen mögliche Großschadenausschläge schützen. Bei einem solchen Rückversicherungsprogramm bleibt zunächst das Risiko, dass ein Ereignis eine Vielzahl von kleinen bis mittleren Schäden innerhalb des Selbstbehalts auslöst. Dieses Exposure (das heißt die Wahrscheinlichkeit, einem Risiko oder Gefahr ausgesetzt zu sein) wird über den Kumulschadenexzedenten an den Rückversicherer transferiert. Risiken, welche sich außerhalb des obligatorischen Rahmens befinden, werden im letzten Schritt, oder vorab, fakultativ rückversichert.

Wird ein Schaden durch ein Ereignis, wie zum Beispiel durch einen Sturm, ausgelöst, so greifen die verschiedenen Rückversicherungsverträge in folgender Reihenfolge ineinander:

1. Die Quotenrückversicherung reduziert die absolute Schadenbelastung durch Teilung der Schäden in einem Verhältnis.
2. Der Schadenexzedent pro Risiko deckt alle einzelnen Schäden, welche die Priorität übersteigen.
3. Unter dem Schadenexzedent pro Ereignis werden alle Schäden eines Ereignisses, welche sich unterhalb der Priorität des Schadenexzedenten pro Risiko befinden, aufaddiert. Der Teil der Summe, welcher die Priorität übersteigt, wird vom Rückversicherer getragen.
4. Schäden, welche fakultative Rückversicherungskapazitäten beanspruchen, werden je nach Vertragsgestaltung proportional oder nicht-proportional vom Rückversicherer beglichen, wobei die fakultative Rückversicherung der Vertragsrückversicherung in aller Regel vorweg geht.

18.3 Einordnung der Rückversicherung in die Industriever sicherung

18.3.1 Risikolandschaft der Industrie aus Perspektive des Rückversicherers

Grundsätzlich lässt sich die Rückversicherung, wie die Erstversicherung, in Versicherungssparten und versicherte Gefahren unterteilen. Hier ist an oberster Stelle die Unterteilung in Lebens- und Nicht-Lebensrückversicherung zu sehen. Die Nicht-Lebensrückversicherung wird international als „Property and Casualty“-Rückversicherung bezeichnet (P&C). Diese Bezeichnung gibt einen Hinweis auf die weitere Unterteilung nach Versicherungssparten im Nicht-Lebensbereich. Denn die folgenden (Rück-)Versicherungssparten werden typischerweise in der traditionellen Rückversicherung unterschieden:

- „Property“: Sach-Rückversicherung, Rückversicherung technischer Versicherung (TV), Transport-Rückversicherung
- „Casualty“: Haftpflichtrückversicherung & Financial-Lines-Rückversicherung

Aus der Perspektive der Industrie spielt eine Vielzahl von Risiken eine signifikante Rolle, welche teilweise nur durch Rückversicherung überhaupt adäquat abgedeckt werden können. Ziel des Erstversicherungsunternehmens ist es, den Industriekunden nach Bedarf gegen seine versicherbaren Risiken zu schützen. Diese können vom Brand innerhalb eines Betriebes bis hin zur persönlichen Haftung der Unternehmensleitungs- und -aufsichtsorgane reichen. Das Industriegeschäft im Besonderen ist im Vergleich zum Privatkundengeschäft deutlich volatiler durch seinen geringeren Ausgleich im Kollektiv und das Bedürfnis nach höheren Versicherungs-/Deckungssummen. Die Größe und Schwere der Risiken sowie das erforderliche Know-how beim Underwriting von Industrierisiken setzen oft voraus, dass der Erstversicherer auf die Kapazitäten und den Service des Rückversicherers

zugreifen kann, um überhaupt geeignete Versicherungsprodukte anbieten zu können. Zu den größten rückversicherbaren Risiken (vgl. Whitehead 2019, S. 16) der Industrie gehören unter anderem:

- Betriebsunterbrechung
- Cyberrisiken
- Naturkatastrophen
- Feuer oder Explosionen
- Umweltrisiken
- Produktrückruf

Im folgenden Abschnitt werden die Herausforderungen für Erst- und Rückversicherer im Rahmen der Rückversicherung des Industriegeschäfts beschrieben. Signifikante Gefahren der Industrie werden den verschieden (Rück-)Versicherungssparten zugeordnet, um so ein Gesamtbild der Rolle des Rückversicherers innerhalb des Industriegeschäfts zu skizzieren. Hierzu wird ausschließlich die Schadensrückversicherung betrachtet. Die Lebensrückversicherung wird nicht behandelt, da der Fokus dieses Kapitels auf die größten versicherbaren Risiken der Industrie gelegt wird. Auch die Unfallrückversicherung wird ausgeklammert. Des Weiteren werden die Grenzen wie auch die Ausschlüsse der Rückversicherung aufgezeigt. Abschließend wird der Mehrwert durch Rückversicherung für Industrikunden dargestellt.

18.3.1.1 Naturkatastrophenauslösende Gefahren

Naturkatastrophen, in der Rückversicherung auch Nat Cat (als Abkürzung für Natural Catastrophes) genannt, sind typischerweise Katastrophen, die durch eine natürlich entstandene, rasche Veränderung der Erdoberfläche oder Atmosphäre entstehen und als Folge eine Auswirkung auf die versicherte Sache haben. Zu den Naturgefahren gehören zum Beispiel meteorologische Ereignisse wie Sturm, Hurrikan, Typhoon, Zyklon, Tornado oder Hagel, hydrologische Ereignisse wie Flut, Tsunami oder Überschwemmung, oder geophysikalische Ereignisse wie Erdbeben oder Vulkanausbruch. Weitere Gefahren sind Dürre, Lawinen, Waldbrand, Epidemien, aber auch der Einschlag von Meteoriten, um ein exotisches Beispiel zu nennen. Zu den bis heute teuersten Naturkatastrophenereignissen zählen der Hurrikan Katrina im Jahre 2005 mit versicherten Schäden in Höhe von 62,2 Milliarden US-Dollar, der Tsunami in Japan in 2011 mit 38 Milliarden US-Dollar und Hurrikan Sandy in 2012 mit 30 Milliarden US-Dollar. Der teuerste Sturm in Deutschland war der Sturm Kyrill im Jahre 2007, der versicherte Schäden in Höhe von damals mehr als zwei Milliarden Euro (nicht indexiert) verursachte (vgl. Heep-Altiner und Berg 2014, S 1 f.).

Besonders durch das hohe regionale Schadenpotenzial eines Ereignisses zählt der Rückversicherungsschutz gegen Naturkatastrophen zu den wichtigsten Funktionen der Rückversicherung. Die Herausforderung für den Erstversicherer ist es, das eigene Versicherungsunternehmen gegen eine Vielzahl von kleinen bis mittleren Schäden, ausgelöst

durch ein Naturkatastrophenereignis, zu schützen. Denn diese Schäden können im Aggregat ein Spitzenrisiko für den Erstversicherer und seine Bilanz darstellen. Im Hinblick auf Industriever sicherung besteht das Risiko darin, dass Naturkatastrophen große Einzelschäden hervorrufen, welche im Erstversicherungsportefeuille neben einer Vielzahl von kleinen Schäden zusätzlich anfallen. Große Einzelschäden entstehen dabei nicht nur aufgrund von Sachschäden an Betriebsgebäuden und Maschinen, sondern die Auswirkungen auf den Betrieb und damit einhergehende Betriebsunterbrechungsschäden können wesentlich zum Schadenausmaß beitragen. Es ist ein deutlicher Trend zu beobachten, dass Betriebsunterbrechungsschäden immer größer und dadurch teurer werden. Gerade in Bezug auf Naturkatastrophen ergibt sich eine signifikante Verteuerung der Betriebsunterbrechungsschäden in der heutigen immer stärker vernetzten Welt und durch „Just-in Time“-Produktion.

Für ein Erstversicherungsunternehmen ist ein solches Schadenereignis oft nicht allein tragbar und wird deshalb an mehrere Rückversicherer weitergegeben. Der Rückversicherer ist mit einem weltweiten Portefeuille gegenüber den meisten Erstversicherungsmärkten besser aufgestellt, um diese regionale Schadenlast aus einem Ereignis auszugleichen. Typischerweise wendet der Erstversicherer eine Kombination aus Einzelschaden- und Kumulschadenexzedenten an, um das Naturkatastrophenrisiko für seinen Bestand zu glätten und zu minimieren.

Der Rückversicherer ist auf die Bewertung solcher Risiken spezialisiert. Neben aufwendigen Simulationen innerhalb mathematischer Modelle setzt der Rückversicherer dabei das Know-how verschiedener wissenschaftlicher Disziplinen ein, wie zum Beispiel aus Meteorologie, Hydrologie oder Geophysik, um die zukünftigen Auswirkungen von Naturgefahren besser erkennen und bewerten zu können und für die angebotenen Rückversicherungslösungen risikoadäquate Prämien zu ermitteln. Weitere wichtige Aspekte innerhalb der Kalkulationen sind die Konzentrationen der Risiken (Kumulkontrolle) innerhalb geografischer Wirkungsbereiche von Naturkatastrophen sowie die zeitliche Begrenzung solcher Ereignisse. Diese Aspekte werden innerhalb der Rückversicherungsverträge genau definiert und abgegrenzt.

18.3.1.2 Man-Made-Katastrophen

Man-Made Katastrophen sind zufällig durch den Menschen oder technisches Versagen ausgelöste Schadenereignisse. Es handelt sich meist um Schäden an Objekten, wie Gebäuden oder Maschinen, mit hohen Versicherungssummen. Beispiele für Man-Made-Katastrophen sind unter anderem Feuer (Brand), Explosion, Implosion, Rauch, Stromausfall, Cyberattacken, Terrorakte, Fahrzeuganprall, Flugzeugabsturz oder der Einsturz von Gebäuden oder Strukturen (vgl. Heep-Altiner und Berg 2014, S. 1 f.). In der Industrie werden die meisten dieser Risiken über die Feuerversicherung und die Transportversicherung abgedeckt, können aber auch innerhalb der Haftpflichtversicherung gedeckt werden. Zusätzlich bieten Pools (Rück-)Versicherungslösungen für typischerweise ausgeschlossene Gefahren, wie zum Beispiel Terror- und Nukleargefahren.

Üblicherweise werden diese Gefahren innerhalb der obligatorischen Rückversicherung durch Einzelschadenexzedenten, Kumulschadenexzedenten und fakultative Rückversicherungslösungen abgedeckt. Grund dafür ist, dass Man-Made-Katastrophen entweder ein einzelnes großes Risiko mit einer hohen Versicherungssumme betreffen oder im kausalen Zusammenhang mehrere Risiken treffen. Gerade im Industriegeschäft ist der Erstversicherer überwiegend hohen Exponierungen durch von Menschen verursachte Schäden ausgesetzt. Zu den teuersten Man-Made-Katastrophen gehören die Terrorattacken vom 11. September 2001 mit einem versicherten Schaden in Höhe von fast 26 Milliarden US-Dollar und die Explosion von Tianjin in China im Jahre 2015 mit einem versicherten Schaden von 1,5 Milliarden US-Dollar.

18.3.1.3 Besondere Aspekte der Sach- und Transportrückversicherung

Sachrückversicherung

Die Sachversicherung, welche im Industriegeschäft als Feuerversicherung bezeichnet wird, bietet grundsätzlich Schutz gegen die in der Police genannten Gefahren an eigenen Sachen wie Gebäuden oder Maschinen. Die Rückversicherung dieser Versicherungssparte ist besonders relevant, da es sich im Rahmen der Industriever sicherung um sehr heterogene Risiken handelt. Im Gegensatz dazu zeichnet der Erstversicherer im Privatkundengeschäft eher homogene Risiken, wie zum Beispiel die Wohngebäude- oder Hausratversicherung. Zeichnet ein Versicherungsunternehmen sowohl Industrie- und Gewerberisiken als auch Privatkundenrisiken müssen die oben genannten Formen der Rückversicherung zur Homogenisierung der Portefeuilles und damit zur Reduzierung der Volatilität angewendet werden. Der Erstversicherer möchte sich durch Rückversicherung einerseits gegen große Einzelschäden, entstehend aus dem Industrie- und Gewerbegeschäft, andererseits gegen eine Kumulierung von Schäden schützen. Daher wird üblicherweise eine Kombination aus einer Einzelschaden- und einer Kumulschadendeckung vereinbart (vgl. Gerathewohl 1976a, S. 73 f.).

Ein Industrieunternehmen signifikanter Größe benötigt oftmals eine Versicherungssumme von mehreren Milliarden Euro. Derartige Kapazitäten werden in der Regel von einer Vielzahl von Erstversicherungsunternehmen durch Mitversicherung, aber auch durch obligatorische Rückversicherung und durch die indirektere Beteiligung fakultativer Kapazitäten durch die Rückversicherungsindustrie getragen. Industrieanlagen sind grundsätzlich Naturkatastrophenrisiken wie auch Risiken von Man-Made-Katastrophen ausgesetzt. Beispielsweise kann neben der Feuergefahr auch das Risiko einer Überflutung einer Industrieanlage eine Rolle spielen. Das Feuerversicherungsgeschäft verlangt eine hohe Flexibilität vom Erstversicherer hinsichtlich der Höhe der Versicherungskapazitäten, der zu versichernden Gefahren und der Bereitschaft, schwerkalkulierbare Risiken in die Portefeuilles aufzunehmen. Dabei nutzt der Erstversicherer Rückversicherung, um seine Versicherungsprodukte so zu gestalten, dass diese den komplexen Ansprüchen der Industrieunternehmen entsprechen können.

Von der klassischen Sachversicherung unterscheiden Erstversicherungsunternehmen zusätzlich noch die technische Versicherung, welche auch separat rückversichert werden

kann. Die Besonderheit der technischen (Rück-)Versicherung ist, dass es sich um den Versicherungsschutz von Maschinen oder gegen Risiken aus dem Bau oder der Errichtung von Gebäuden handelt. Auf Grund dessen werden über diese Sparte überwiegend Risiken der Industrie oder des Gewerbes angenommen. Auch diese Risiken sind hoch exponiert und erfordern sowohl die Kapazitäten als auch das Know-how des Rückversicherers, um sie innerhalb der Portefeuilles des Erstversicherers tragbar zu machen. Ein Ausgleich durch homogenes Privatkundengeschäft findet nicht statt.

Transportrückversicherung

Unter dem Begriff der Transportrückversicherung wird zum einen der Transfer von Großschäden während des Transports an Gütern und Waren, zum anderen von Eigenschäden am Transportmittel auf den Rückversicherer verstanden. Des Weiteren werden im deutschen Versicherungsmarkt auch andere speziellere Versicherungssparten, wie zum Beispiel gegen Kidnap & Ransom (Entführung und Erpressung) oder die Veranstaltungsausfallrückversicherung, unter diesem Begriff zusammengefasst. Da diese Risiken sehr unterschiedlicher Natur sind, werden üblicherweise separate Rückversicherungsverträge vereinbart. Die Transportrückversicherung teilt überwiegend die Gefahren der Sachrückversicherung und schützt den Erstversicherer im Einzelschadenfall. Neben der Feuerrückversicherung ist die Transportrückversicherung eine der wichtigsten Rückversicherungssparten für Industriekunden, denn mit der zunehmenden Globalisierung und Vernetzung geht eine wachsenden Bedeutung der Waren- und Gütertransporte als Teil der Wertschöpfungskette einher (vgl. Gerathewohl 1976b, S. 415 f.).

18.3.1.4 Besondere Aspekte der Haftpflichtrückversicherung

Die Haftpflichtrückversicherung schützt den Erstversicherer vor Großschäden ausgelöst durch zivilrechtliche Schadenersatzansprüche geschädigter Dritter. Neben Industrie-, Gewerbe- und Privatkundengeschäft wird dabei auch zwischen verschiedenen Versicherungsprodukten differenziert. Für Industrieunternehmen sind hierbei bedeutende Haftpflichtversicherungsprodukte die Kraftfahrthaftpflichtversicherung innerhalb einer Flotte, die Arbeitgeberhaftpflichtversicherung, die Betriebshaftpflichtversicherung, die Produkthaftpflichtversicherung, die Vermögensschadenhaftpflichtversicherung und die D&O-Versicherung.

Hierbei kann jeweils ein separates Rückversicherungsprogramm pro Untersparte oder eine Zusammenfassung mehrerer Untersparten für Industriever sicherungsprodukte und/oder Privatkundenprodukte vereinbart werden. Auch in der Haftpflichtversicherung unterscheiden sich die Portefeuilles der Privat- und Industriekunden stark. Sind die Versicherungssummen im Privatkundengeschäft weitestgehend gleich, werden im Gegensatz dazu innerhalb des Industriegeschäfts die Kapazitäten des Erst- und Rückversicherers stärker beansprucht. Besonders hervorzuheben sind die Produkthaftpflicht-, die Betriebshaftpflicht- und die D&O-Versicherung, welche durch ihre besondere Risikoexponierung Großschäden auslösen können. Der Erstversicherer kann sich dabei nur bedingt gegen eine Kumulierung von Haftpflichtschäden schützen. Auch ist das gesetzli-

che und regulatorische Veränderungsrisiko groß und betrifft eine Vielzahl verschiedener Haftpflichtrisiken. Vorwiegend wird in der Haftpflichtrückversicherung der einzelne (Teil-)Schaden an den Rückversicherer transferiert. Dadurch eignet sich auch in diesen Sparten ein Rückversicherungsprogramm auf Basis eines Einzelschadenexzedenten, welches eine Komponente zur Absicherung gegen mögliche Kumulierungen innerhalb des Portefeuilles umfasst (vgl. Gerathewohl 1976b, S. 307 f.).

18.3.1.5 Ausschlüsse der Vertragsrückversicherung und Spezialakzepte

Zu den generellen Ausschlüssen der Vertragsrückversicherung gehören die folgenden Gefahren:

Kriegsgefahr

Krieg und kriegsähnliche Ereignisse innerhalb des geografischen Geltungsbereichs des obligatorischen Rückversicherungsvertrags sind üblicherweise ausgeschlossen. Jedoch ist dies auch im Erstversicherungsvertrag überwiegend der Fall, sodass keine Deckungslücke zwischen Erst- und Rückversicherung besteht.

Terrorgefahr

Auch die Terrorgefahr wird in obligatorischen Rückversicherungsverträgen ausgeschlossen. Dieser Ausschluss gewann nach den Terroranschlägen vom 11. September 2001 an zusätzlicher Bedeutung. In Deutschland besteht seither für (Erst-)Versicherungsnehmer die Möglichkeit, diese Gefahr über einen Pool (Extremus AG) separat abzusichern, für den ab einer gewissen Grenze der Staat haftet. Auch bietet Lloyds of London gegen Terroristen (Erst-)Versicherungskapazitäten an.

Nukleargefahr

Innerhalb der sogenannten Nuklearausschlüsse wird zwischen ursachenbezogenen und anlagenbezogenen Ereignissen unterschieden. Zum einen wird das Risiko eines Schadens, ausgelöst durch Nukleargefahren, auf dem Betriebsgelände und daraus entstehende Haftpflichtschäden Dritter ausgeschlossen, zum anderen werden alle ursachenbezogenen Ereignisse, wie die Nutzung von radioaktivem Material, innerhalb der Medizin oder anderer industrieller Bereiche ausgeschlossen. Üblicherweise werden hier international gültige Standardklauseln vereinbart. Betreiber von Atomkraftwerken haben die Möglichkeit, sich über entsprechende Pools abzusichern.

Cybergefahren und IT-Ausschlüsse

Ein weiterer allgemeiner Ausschluss in Rückversicherungsverträgen kann der Ausschluss von Schäden entstanden durch Cyberattacken bzw. die Realisierung von IT-Risiken sein. Dieses Risiko kann seit längerem über die neu entwickelte Cyberversicherungssparte versichert und dann auch eigenständig rückversichert werden und wird inzwischen zunehmend innerhalb von Sach-, Transport- und Haftpflichtrückversicherungsverträgen ausgeschlossen. Dieses Vorgehen wird im Erst- und Rückversicherungsmarkt unter dem

Stichwort „Silent Cyber“ diskutiert. Ein Beispiel hierfür ist eine erfolgreiche Cyberattacke auf einen Staudamm, welche zur Überflutung eines Gebietes führt. Der entstandene Flutschaden wäre über die Kumulschadendeckung des Sachrückversicherungsvertrages auf den Rückversicherer transferiert, wenn im Rückversicherungsvertrag kein entsprechender Ausschluss vereinbart wurde.

Weitere Ausschlüsse und Spezialakzepte

Neben den oben genannten können regelmäßig noch weitere Ausschlüsse innerhalb eines Rückversicherungsvertrages vereinbart sein. Beispielsweise werden Risiken aus anderen obligatorischen Rückversicherungsverträgen ausgeschlossen, um die Transparenz der Portefeuilles zu gewährleisten. Des Weiteren werden grundsätzlich die Gefahren und Risiken von den Rückversicherungsvertrag nicht betreffenden Sparten ausgeschlossen. Dies bedeutet, dass zum Beispiel in Sachrückversicherungsverträgen die Zession reiner Haftpflichtrisiken ausgeschlossen sein kann.

Außerdem kann der Erstversicherer auf zusätzliche Deckungserweiterungen innerhalb des obligatorischen Rückversicherungsvertrags, sogenannte Spezialakzepte, zurückgreifen. Diese erweitern für einzelne benannte Risiken den obligatorischen Rahmen der Vereinbarung und erlauben es, inhaltliche Deckungserweiterungen, wie zum Beispiel einen zusätzlichen geografischen Geltungsbereich für ein einzelnes Risiko, ohne Nutzung fakultativer Rückversicherung mit in den obligatorischen Rückversicherungsvertrag aufzunehmen. Ein Vorteil ist, dass Spezialakzepte meist keine Auswirkung auf den Preis des bestehenden Rückversicherungsvertrages haben und wenig administrativen Aufwand erzeugen.

18.3.1.6 Grenzen der fakultativen Rückversicherung und nicht-rückversicherbare Risiken

Die fakultative Rückversicherung bietet dem Erstversicherer die Möglichkeit, außergewöhnliche Risiken seiner Bestände weiter an den Rückversicherer zu zedieren. Grundsätzlich ist jedes Risiko versicherbar, solange der Preis dem Risiko entspricht und Kriterien wie Zufälligkeit und Unvorhersehbarkeit erfüllt sind. So ist der (Rück-)Versicherungsmakler Lloyds of London auf die Zeichnung außergewöhnlicher Risiken spezialisiert, welche durch besonders hohe Versicherungswerte oder durch eine außergewöhnliche Gefahrexponierung gekennzeichnet sind. Jedoch wird nicht jedes Risiko eines Versicherungsnehmers, besonders im Industriegeschäft, vom Erstversicherer gezeichnet. Großschäden, welche zur Kalkulation der Prämie herangezogen werden, treten selten auf und bieten daher nicht immer eine geeignete Basis zur Prämienberechnung. Außerdem kann es für den Erst- und auch Rückversicherer schlachtweg unprofitabel sein, zu stark exponierte Risiken zu zeichnen. Denn solche Risiken zeigen in einer Vergangenheitsbetrachtung meist schlechte Schadenverläufe. Selbst wenn der Rückversicherer bereit ist, das Risiko in seinen Bestand aufzunehmen, müssen Erstversicherer und Versicherungsnehmer damit rechnen, dass die (Rückversicherungs-)Prämie dem Schadenverlauf entsprechend sehr hoch und möglicherweise unattraktiv ist.

Obwohl die Rückversicherung viele Möglichkeiten zur Übernahme großer Risiken und damit einhergehender Gefahren bietet, existieren darüber hinaus weitere Gefahren für die Industrie, welche (bislang) nicht vom Rück- und damit zumeist auch nicht vom Erstversicherer übernommen werden. Ein zuvor genanntes Beispiel ist die Gefahr des Krieges oder kriegsähnlicher Ereignisse, welche grundsätzlich aus Verträgen ausgeschlossen sind. Auch unvorhergesehene systemische Risiken, wie die Veränderung der politischen oder rechtlichen Lage eines Landes und die damit verbundenen Auswirkungen für ein Unternehmen werden regelmäßig nicht von der (Rück-)Versicherungsindustrie übernommen. Ein Beispiel hierfür sind die negativen Auswirkungen von Handelssanktionen. Werden diese von Ländern verhängt, besteht selbst für Erst- und Rückversicherer keine Möglichkeit, vertraglich vereinbarte Leistungen, wie die Entschädigung eines Schadens, zu erbringen. Eine weitere Gefahr in diesem Zusammenhang ist die steigende Bedrohung durch den Klimawandel: Die Entwicklung und die Kalkulation von Prämien ist weitestgehend abhängig von Schadenverläufen der Vergangenheit. Vor diesem Hintergrund ist es schwierig, eine für diese, bislang historisch nicht oder nur schwer mit Schadendaten belegbare, Risikolage adäquate Prämie zu kalkulieren. Gleichwohl bezieht der Rückversicherer die steigende Gefahr durch den Klimawandel mit in seine Kalkulationen ein. Auch Gefahren im Zusammenhang mit der Digitalisierung im Allgemeinen oder mögliche Folgen eines Hackerangriffs im speziellen sind nicht vollumfänglich versicherbar. Beispielsweise sind die Auswirkungen eines Reputationsverlustes durch den Verlust personenbezogener Daten nur schwer quantifizierbar. Und auch weitere Systemrisiken, wie zum Beispiel aus der Volatilität bestimmter Märkte, aus Bedrohungen durch M&A-Aktivitäten oder durch einen Crash der Finanzmärkte, lassen sich nicht oder nur eingeschränkt auf die Versicherungsindustrie transferieren. Abschließend sei hierzu angemerkt, dass die genannten, nicht (rück)versicherungsfähigen Risiken ggf. durch ein geeignetes Risikomanagement im Industrieunternehmen selbst reduziert oder gar vermieden werden können. Insofern ist eine Kombination aus Risikomanagement des Industrikunden, aus Transfer der hierfür geeigneten Risiken auf die Bilanz des Erstversicherers und schließlich aus der Übernahme von Risikospitzen durch den Rückversicherer gefragt, um hierdurch eine möglichst optimierte Absicherung der (Versicherungs-)Risiken eines Industrieunternehmens zu gewährleisten.

18.3.2 Mehrwert der Rückversicherung für Industrikunden

Die meisten Erstversicherer, die das Industriesegment betreiben, sind nicht vollumfänglich global aufgestellt. Zwar haben sich Erstversicherungskonzerne gerade im letzten Jahrzehnt deutlich vergrößert und insbesondere auch durch entsprechende M&A-Aktivitäten international erweitert. Jedoch bleibt weiterhin die langjährige, gerade auch internationale Erfahrung der Rückversicherungsbranche für eine erfolgreiche Bewertung und damit auch Zeichnung von Industriegeschäft wichtig. Die Versicherungstechnik lebt nach dem „Gesetz der großen Zahlen“, also dem Ausgleich im Kollektiv der Versicherten und in der Zeit. Dafür sind die Schaden- und Portfoliodaten wichtig, die gerade der Rückversicherungsmarkt

branchen- und segmentspezifisch im Industriesegment besonders gut beisteuern kann, da für Rückversicherer der Risikoausgleich auf internationaler Ebene stattfindet. Daher ist das Zusammenspiel von Erst- und Rückversicherungsmarkt für einen optimal konzipierten und ausgesteuerten Risikotransfer im Industriegeschäft sehr wichtig. Die langjährige Erfahrung und der globale Blickwinkel der Rückversicherungsbranche bringt Mehrwert und Nutzen für den Erstversicherer und somit letztlich auch für den Industrikunden.

Beispiele, die dies belegen, gibt es viele. Aus dem Eigenschadenbereich sei hier die Deckung on Offshore-Windparks erwähnt. Solche, meist auch „Prototyp“-Projekte benötigen viele kapitalstarke Versicherungspartner mit technischem Know-how. Die Rückversicherungsbranche begleitet hierbei die Entwicklung von Versicherungslösungen mit Ingenieurwissen und unterstützt bei der Zusammenstellung der benötigten Deckungskapazitäten. Das Wissen und die Erfahrung aus den diversen, zum Beispiel in der Nordsee bereits realisierten Projekten werden nun auch in Asien und zukünftig in anderen Teilen der Erde abgefragt. Dabei ist die Versicherung solcher Projekte häufig eine Voraussetzung, dass die Umsetzung finanziell überhaupt realisierbar ist. Die Rückversicherungsbranche ist hieran maßgeblich beteiligt.

Aus dem Fremdschadenbereich kann ein weiteres Beispiel für ein deutsches Produkt bemüht werden: innovative Küchenmaschinen, welche seit einigen Jahren in vielen deutschen Haushalten einziehen und traditionell nur von Unternehmen in den heimischen oder europäischen Märkten vertrieben werden. Entscheidet sich ein Unternehmen, ein solches Produkt zu entwickeln und zu vertreiben, welches dann auch im Ausland, zum Beispiel in den USA verkauft werden soll, dann muss unbedingt eine Erweiterung der Produkthaftpflichtversicherung für Exporte in die USA vereinbart werden. Nicht jeder Erstversicherer ist mit den Gesetzen und staatenspezifischen Regelungen in dieser Region ausreichend vertraut. Hierbei kann dann der Rückversicherer mit seinen Experten in Haftungs- und Deckungsfragen und mit Erfahrungen in der Schadenabwicklung über eigene Experten und/oder die Empfehlung entsprechender Sachverständiger und Anwälte unterstützen.

Des Weiteren verfügen Rückversicherer meist über ein hohes (Solvenz-)Kapital, woraus folgt, dass ausreichend hohe Zeichnungskapazitäten zur Verfügung gestellt werden können. Rückversicherer akzeptieren regelmäßig große und komplexe Risiken, wozu zum Beispiel auch Prototyp-Risiken gehören, die im Zuge des sehr schnellen technischen Fortschritts weiter an Bedeutung gewinnen. In Summe ist der Rückversicherer also darauf spezialisiert, gerade die (internationalen) Risiken der Industrie zu zeichnen bzw. den Erstversicherer bei der Zeichnung dieser Risiken zu begleiten, indem er mit Erfahrung und Expertenwissen unterstützt. Erstversicherungsunternehmen, welche internationale Versicherungslösungen anbieten, sind deswegen für ein stimmiges Underwriting und das Entwickeln passgenauer Deckungslösungen häufig auf die Kapitalstärke und Expertise des Rückversicherers angewiesen. Somit bietet die Rückversicherung einen besonderen Mehrwert, sowohl für den Erstversicherer als auch für die Industrie, da sie den Transfer industrieller Risiken in den Versicherungsmarkt überhaupt erst ermöglicht.

Ein weiterer Mehrwert ist der Service, welcher dem Erstversicherer vom Rückversicherer zur Verfügung gestellt wird. Dieser umfasst zu einem die Unterstützung bei der Erstellung von Deckungskonzepten von komplexen Risiken, zum anderen aber auch die Bereitstellung von Informationen, wie zum Beispiel Naturgefahrenkarten oder Online-Portale, über die sich lokationspezifisch die Gefährdungslage für bestimmte Risiken einsehen lässt. Weitere Beispiele sind die Preisfindung, die Unterstützung bei der Einführung neuer Versicherungsprodukte oder die Beurteilung neuer Gefahren, wie zum Beispiel Cyber. Im Servicebereich kann der Rückversicherer insbesondere sein internationales Know-how zeigen. Neben Underwriting-Spezialisten aus den einzelnen Versicherungssparten setzt der Rückversicherer dabei auch auf Expertise aus anderen Fachbereichen. Beispiele hierfür sind Meteorologen, Geologen, Mathematiker oder Rechtsanwälte, mit deren Hilfe mögliche zukünftige (Katastrophen) Schadenszenarien bewertet werden können. Hier zielt der Rückversicherer darauf ab, sowohl die Eintrittswahrscheinlichkeit als auch die Höhe der möglichen Schäden zu antizipieren. Besonders ist die Bewertung möglicher Naturkatastrophenschadenszenarien zu erwähnen. Innerhalb der sogenannten Naturkatastrophenmodellierung werden nämlich Erkenntnisse mehrerer wissenschaftlicher Disziplinen miteinander kombiniert, um dann in einem mathematischen Modell Aussagen zu möglichen Katastrophenszenarien treffen zu können. Der Rückversicherer spielt also eine besondere Rolle bei der Zeichnung von Industrierisiken. Mithilfe der Rückversicherung sind Erstversicherer häufig erst fähig, der Industrie maßgeschneiderte Versicherungslösungen anzubieten. Durch die Bereitstellung zusätzlicher Kapazität, der Beratung des Erstversicherers im Rahmen von Services und der Übernahme von Kumul- und Großschäden ist Rückversicherung ein wichtiger Bestandteil des Risikotransfers zwischen Industrikunden und Erstversicherungsunternehmen.

18.4 Fazit

In diesem Kapitel wurde die Rolle des Rückversicherers innerhalb der Industriever sicherung dargestellt. Nach einem kurzen Überblick über den nationalen und internationalen Rückversicherungsmarkt wurden die Grundlagen der traditionellen Rückversicherung erläutert. Es wurde herausgestellt, wie die verschiedenen Rückversicherungsarten und -formen den Risikotransfer industrieller Risiken ermöglichen und wie dies in verschiedenen Industriever sicherungssparten erfolgt. Des Weiteren wurden die üblichen Ausschlüsse typischer Rückversicherungsverträge beschrieben, um im anschließenden Abschnitt die Grenzen der obligatorisch- und fakultativen Rückversicherung aufzuzeigen. Abschließend wurde der besondere Mehrwert der Rückversicherung gerade für Industrikunden herausgearbeitet.

Mit Blick auf die Zukunft der traditionellen Rückversicherung ist festzustellen, dass der Risikotransfer an Rückversicherungsunternehmen, gerade in Bezug auf die voranschreitende Globalisierung, ein immer bedeutenderes Instrument wird, um bei der Absi-

cherung großer Einzelschäden eines Industrieunternehmens oder auch der Versicherung von Naturkatastrophenereignissen den geeigneten Zugang zu globalem Kapital und zu den benötigten Versicherungskapazitäten zu ermöglichen.

Literatur

- AON. (2019). Reinsurance Market Outlook January 2019. AON security Inc. 2019. <http://thought-leadership.aonbenfield.com/pages/Home.aspx?ReportCategory=Reinsurance%20Market%20Outlook>. Zugegriffen am 30.06.2019.
- Bevere, L., Schwartz, M., Sharan, R., & Zimmerli, P. (2018). Swiss Re Sigma No 1/2018 Natural catastrophes and man-made disasters in 2017: A year of record-breaking losses. Swiss Re Management Ltd. https://www.swissre.com/dam/jcr:1b3e94c3-ac4e-4585-aa6f-4d482d8f46cc/sigma1_2018_en.pdf. Zugegriffen am 30.06.2019.
- Bundesanstalt für Finanzdienstleistungsaufsicht. (2018). 2017/2018 Statistik der Bundesanstalt für Finanzdienstleistungsaufsicht – Rückversicherungsunternehmen-. Bundesanstalt für Finanzdienstleistungsaufsicht. https://www.bafin.de/DE/PublikationenDaten/Statistiken/Rueckversicherung/rueckversicherung_artikel.html. Zugegriffen am 30.06.2019.
- Gerathewohl, K., Bauer, W., Glotzmann, P., Hosp, E., Klein, J., Kluge, H., & Schimming, W. (1976a). *Rückversicherung Grundlagen und Praxis Band I*. Karlsruhe: Versicherungswirtschaft e. V.
- Gerathewohl, K., Bauer, W., Glotzmann, P., Hosp, E., Klein, J., Kluge, H., & Schimming, W. (1976b). *Rückversicherung Grundlagen und Praxis Band II*. Karlsruhe: Versicherungswirtschaft e. V.
- Heep-Altiner, M., & Berg, M. (2014). Katastrophenmodellierung – Naturkatastrophen, Man Made Risiken, Epidemien und mehr, Proceedings zum 6. FaRis & DAV Symposium am 13.06.2014 in Köln, Institut für Versicherungswesen/Institute for Insurance Studies. https://cos.bibl.th-koeln.de/frontdoor/deliver/index/docId/51/file/6_2014.pdf. Zugegriffen am 30.06.2019.
- Liebwein, P. (2018). *Klassische und moderne Formen der Rückversicherung*. Karlsruhe: VVW GmbH.
- McKinsey & Company. (2017). Global reinsurance: Fit for the future? McKinsey & Company. <https://www.mckinsey.com/industries/financial-services/our-insights/global-reinsurance-fit-for-the-future>. Zugegriffen am 30.06.2019.
- Schwepcke, A. (2004). *Rückversicherung Grundlagen und aktuelles Wissen – Ein Leitfaden zum Selbststudium*. Karlsruhe: Versicherungswirtschaft GmbH.
- Sheehan, M. (2018). Munich Re moves top in A.M. Best's 2018 reinsurance rankings. *Reinsurance News*. <https://www.reinsurancene.ws/munich-re-recovers-top-spot-in-a-m-best-s-2018-reinsurance-rankings/>. Zugegriffen am 30.06.2019.
- Whitehead, J. (2019). Allianz risk barometer top business risks for 2019 – The most important corporate perils for the year ahead and beyond, based on the insight of more than 2,400 risk management experts from over 80 countries. Allianz Global Corporate & Specialty SE. <https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf>. Zugegriffen am 30.06.2019.

Angelika Trotta ist International Chief Underwriter für das fakultative Property Geschäft. Sie absolvierte eine Ausbildung beim Gerling-Konzern und ein Studium zur Diplom Kauffrau an der TH Köln. Anschließend war sie bei einem großen Maklerhaus zuständig für die Koordination internationaler Versicherungsprogramme. Seit 1994 ist sie bei der Gen Re für das fakultative Sach/TV und

Transport-Geschäft in verschiedenen Leitungspositionen tätig. Schwerpunkt ihrer Tätigkeit sind Grundsatzfragen/Underwriting Policy, Portfolio-Steuerung und Kapazitätsmanagement für EMEA, Afrika, Asien, Australien, Neuseeland sowie Mittel- und Südamerika als auch Training und Coaching junger Underwriter.

Jan Fischer studierte dual Versicherungswesen mit den Schwerpunkten Rückversicherung, Bilanzierung von Versicherungsunternehmen und HUKR (Haftpflicht-, Unfall-, Kraftfahrt-, und Rechtsschutzversicherung) am Institut für Versicherungswesen der Technischen Hochschule Köln. Im Anschluss absolvierte er dort auch das Masterstudium Risk & Insurance und war gleichzeitig als Werkstudent im Bereich Rückversicherung tätig.



Alternativer Risikotransfer

19

Ralf Weyand und Mathis Herzke

Zusammenfassung

Durch eine sich immer schneller verändernde Risikolandschaft, technologischen Fortschritt und die Globalisierung zeigen sich auch die Grenzen der Kapazität des Versicherungsmarktes. Um diese Kapazitäten zu erhöhen, wurden Methoden entwickelt, die eine Einbeziehung des Finanzmarktes ermöglichen. Diese Methoden werden aufgrund ihrer unterschiedlichen Charakteristika als alternativer Risikotransfer bezeichnet. Alternativer Risikotransfer gewinnt immer mehr an Bedeutung. Durch die erhöhte Frequenz von Naturkatastrophen, das Niedrigzinsniveau sowie durch Ineffizienzen des Versicherungsmarktes sind die Rahmenbedingungen für eine weitere positive Entwicklung alternativen Risikotransfers günstig. In diesem Kapitel werden eine Eingliederung der verschiedenen Instrumente des Alternativen Risikotransfers vorgenommen, die verschiedenen Instrumente vorgestellt und abschließend ein Fazit und ein Ausblick für die weitere Entwicklung gegeben.

19.1 Einleitung

Die globale Risikolandschaft befindet sich in einem beständigen und mit zunehmender Geschwindigkeit stattfindenden Wandel. U. a. durch technologischen Fortschritt, stärkere Regulierung, internationale Verflechtungen und steigende Wertkonzentration werden neu-

R. Weyand (✉)

Hannover Rück SE, Hannover, Deutschland

E-Mail: Ralf.Weyand@hannover-re.com

M. Herzke

TH Köln, Institut für Versicherungswesen, Köln, Deutschland

E-Mail: mathis.herzke@web.de

artige Risikokonzepte zur Absicherung der entstehenden Risiken benötigt. Besonders die erhöhte Frequenz und das wachsende Schadenpotenzial von Naturkatastrophen stellt die Versicherungsbranche aktuell vor große Herausforderungen. So zeigen vor allem Hurrikans und Erdbeben die Kapazitätsgrenzen der Versicherungsbranche auf. Obwohl die einzelnen Ereignisse nicht unbedingt stärker sind als in der Vergangenheit, steigen die Schadenpotenziale durch die erhöhte Wertekonzentration und die steigende Frequenz deutlich.

Zusätzlich zu der Veränderung der Risikolandschaft finden auch in der Risikoträgerlandschaft durch Wettbewerb, Mergers & Acquisitions und Marktaustritte ständige Umgestaltungen, sowohl auf dem Erst- wie auch auf dem Rückversicherungsmarkt, statt. Diese können für die Unternehmen einer Branche erhebliche Auswirkungen auf die Deckungskapazitäten und Prämien, die auf dem Versicherungsmarkt angeboten werden, haben, wie zum Beispiel die Austritte einiger Versicherer aus dem Krankenhaus-Haftpflichtgeschäft zeigen.

Ein weiterer maßgeblicher Grund für die Veränderung der Risikoträgerlandschaft ist die anhaltende Niedrigzinsphase. Durch die bewusst niedrig gehaltenen Zinsen werden Erst- und Rückversicherer dazu gezwungen, technisch auskömmliche Raten zu erzielen, da eventuelle Abweichungen der Schadenkalkulation nicht, wie früher, durch hohe Zins-einnahmen ausgeglichen werden können.

Ebenfalls aufgrund der niedrigen Zinsen werden durch die vergleichsweise attraktiven Renditen Finanzmarktinvestoren auf den Versicherungsbereich aufmerksam und entschließen sich, vermehrt auf diesem zu investieren. Die Grundlage für diesen Befund bildet die steigende Konvergenz zwischen dem Kapital- und dem Versicherungsmarkt, welche die Entwicklung neuer Instrumente zur Risikoabsicherung ermöglicht.

Um die Ineffizienzen und Kapazitätsbeschränkungen des klassischen Versicherungsmarktes zu vermeiden oder zu umgehen, wurden verschiedene Methoden entwickelt. Diese Methoden können den Kapitalmarkt, andere Unternehmensstrukturen oder verschiedene Absicherungsmöglichkeiten berücksichtigen. Aufgrund der unterschiedlichen Ansätze im Vergleich zu traditionellen Versicherungslösungen werden diese Instrumente unter dem Begriff „Alternativer Risikotransfer“ (ART) zusammengefasst (vgl. Liebwein 2009, S. 431–432).

19.2 Alternativer Risikotransfer

19.2.1 Definition Alternativer Risikotransfer

Der Begriff „Alternativer Risikotransfer“ (ART) ist bis heute nicht allgemeingültig definiert. Dies führt in der Praxis zu einem unpräzisen Umgang mit diesem Begriff. Allerdings besteht eine breite Einigkeit, dass sich der Terminus „Alternativ“ auf die Einbeziehung von Finanzmärkten für den Transfer von versicherungstechnischen Risiken als Alternative zum Versicherungsmarkt bezieht. Alternativer Risikotransfer ist zusätzlich zum traditionellen Risikotransfer auf dem Erst- und Rückversicherungsmarkt zu sehen. Es wird damit

ein Spektrum an Produkten bezeichnet, welches den traditionellen Versicherungsprodukten (Erst- und Rückversicherung) als Ergänzung, aber nicht notwendigerweise als Ersatz gegenübersteht (vgl. Kuck 2000, S. 58). Die Elemente des Alternativen Risikotransfers müssen, wie bei traditionellen Versicherungslösungen, nicht in Reinform verwendet werden, sondern können auch untereinander kombiniert werden (vgl. Schwepcke et al. 2017, S. 142).

Alternativer Risikotransfer kann sich von traditionellen (Rück-)Versicherungsformen durch den Umfang der transferierten versicherungstechnischen Risiken (Art des Ausgleichsmechanismus), die Art des aktivierenden Events (das auslösende Ereignis der Zahlung), die Art des transferierten Risikos (zum Beispiel neuartige oder seltene Risiken, für die der Ausgleich im Kollektiv nicht vorliegt) sowie der Art des Risikoträgers (zum Beispiel Selbsttragung oder Übertragung auf den Kapitalmarkt) unterscheiden (vgl. Schwepcke et al. 2017, S. 141).

Ein eingrenzender Faktor innerhalb der breiten Definition Alternativen Risikotransfers ist, dass Alternativer Risikotransfer als Hauptaufgabe primär den Transfer versicherungstechnischer Risiken und somit das Erreichen versicherungstechnischer Ziele mithilfe des Kapitalmarktes hat. Abwandlungen von klassischer Rückversicherung (zum Beispiel strukturierter Rückversicherung) konzentrieren sich eher auf das Erreichen gesamtbehaf-fter Ziele mithilfe versicherungstechnischer Instrumente (vgl. Liebwein 2018, S. 474).

Ein Grund für die unklare Verwendung des Begriffes kann darin gesehen werden, dass neue Entwicklungen beim Risikotransfer häufig unter dem Begriff „Alternativer Risikotransfer“ zusammengefasst werden. Dies hat zur Folge, dass auch Produkte, die eher einer Risikofinanzierung dienen als einem Risikotransfer, unter dem Begriff Alternativer Risikotransfer verstanden werden (vgl. Flämig 2007, S. 1). Eine in der Literatur übereinstim-mende Gliederung der unterschiedlichen Ausprägungsformen Alternativen Risikotransfers ist aufgrund der unklaren Abgrenzung und Definition des Themas nicht vorhanden.

Der Begriff des Alternativen Risikotransfers wird in diesem Kapitel als Oberbegriff für nicht-klassische Versicherungslösungen gesehen. Die Struktur von Alternativem Risiko-transfer wird in diesem Kapitel in Kapitalmarktprodukte, Rückversicherungsprodukte und Mischformen (hybride Instrumente) unterteilt (vgl. Abb. 19.1).

19.2.2 Alternativer Risikotransfer – Geschichte und Zielsetzung

Aufgrund der unklaren und weit gefassten Definition sowie der stufenhaften und noch nicht abgeschlossenen Entwicklung von ART ist es nicht möglich, eine genaue Bestim-mung des Ursprunges festzustellen. Tatsache ist, dass sich innerhalb des letzten Jahrhun-derts die Ansprüche an den Erst- und Rückversicherungsmarkt stark verändert haben. Als Folge dieser Veränderung hat sich ART entwickelt. Der Beginn von ART wird von diver-sen Quellen im 19. Jahrhundert angesiedelt, als das erste Mal eine Captive, ein unterneh-menseigener Versicherer, eingesetzt wurde (vgl. Young 1991, S. 15 ff.).

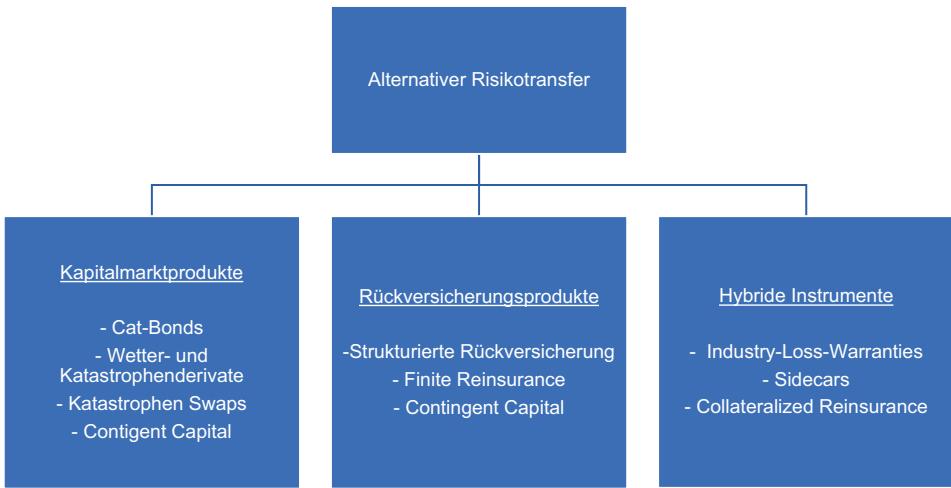


Abb. 19.1 Grundstruktur des Alternativen Risikotransfers. (Quelle: eigene Darstellung in Anlehnung an Cummins et al. 2009, S. 506)

Die folgende Entwicklung und Ausprägung von weiteren Konzepten des Alternativen Risikotransfers hängt mit der starken Zunahme von Schadenpotenzialen zusammen. Dies resultiert aus der steigenden Frequenz von Schadensfällen und einer Entwicklung der Schadenhöhen bei Naturkatastrophen sowie aus fehlender Wirtschaftlichkeit bei der Versicherung neuartiger und bekannter Risiken auf dem traditionellen Versicherungsmarkt.

Die Notwendigkeit zusätzlichen Kapitals innerhalb der Versicherungsbranche wurde erstmals 1992 deutlich, als Hurrikan „Andrew“ Florida und die Küste des Golfs von Mexiko heimsuchte. Verursacht wurden Schäden in Höhe von 27 Milliarden US-Dollar, von denen 15,5 Milliarden US-Dollar versichert waren. Aufgrund dieser Schadenbelastung mussten acht Versicherungsunternehmen Insolvenz anmelden und weitere standen kurz vor der Insolvenz. Um dieses in Zukunft zu vermeiden, versuchten Versicherungsunternehmen, mehr Rückversicherungsschutz am Markt einzukaufen, um sich abzusichern. Dies zeigte auf, dass mehr Kapital in den Rückversicherungsbereich fließen musste, um zusätzliches Kapital bereitzustellen (vgl. Polacek 2018, S. 1). Als erste Verbrieftung von Versicherungsrisiken am Kapitalmarkt wurde die Cat-Bond-Transaktion „Kover“ der Hannover Rück im Jahre 1994 vollzogen. Bei dieser Transaktion wurde mithilfe eines Special-Purpose Vehicle (SPV) die Quotenabgabe eines bestimmten Portfolios auf den Finanzmarkt übertragen. Das Investitionsvolumen betrug 85 Millionen US-Dollar (vgl. Zeller 2008, S. 7).

Einen zusätzlichen Entwicklungsschub für ART ergab der zwingende Handlungsbedarf aus diversen Krisen in der Versicherbarkeit von Risiken und entsprechender Kapazitätsbereitstellung. Ein Beispiel ist die fehlende Versicherbarkeit im Bereich der Haftpflichtabsicherung aufgrund der Höhe gesetzlich ermöglichter Schadenersatzforderungen im

medizinischen Bereich. Dies war insbesondere in den 1970er Jahren für ärztliche Behandlungsfehler in den Vereinigten Staaten von Amerika der Fall (vgl. Eickstädt 2001, S. 71 f.).

Bedingt durch den technischen Fortschritt und die Urbanisierung haben sich zunehmend steigende Vermögenswerte in Gebieten entwickelt, die durch Naturkatastrophen gefährdet sind. Dies hat zur Folge, dass die heutigen Naturkatastrophen ein deutlich höheres Schadenpotenzial besitzen, als vergleichbare Ereignisse in der Vergangenheit (vgl. Cummins et al. 2009, S. 494–496). Der versicherte Schaden des Hurrikans „Katrina“ im Jahr 2005 wurde schon auf mehr als 62 Milliarden US-Dollar beziffert (vgl. Polacek 2018, S. 3).

Ein weiterer unterstützender Faktor für die Entwicklung von ART war das periodenweise wechselnde Zeichnungsverhalten der Rückversicherungsbranche. So waren zeitweise sogenannte „Soft Markets“ (weiche, das heißt einkäuferfreundliche Märkte) vorhanden, die sich durch flexible Preise und vorhandene Kapazitäten für Erstversicherungsrisiken ausgezeichnet haben. Ebenfalls temporär sind auch sogenannte „Hard Markets“ (harte Märkte) vorhanden, bei denen die Preise für die Absicherung relativ hoch waren und/oder die angebotene Deckung begrenzt war. Aufgrund der geringen Korrelation zwischen dem periodenweisen Underwriting der Rückversicherungsbranche und dem Finanzmarkt kann ART für die Versicherer und Versicherten einen Mehrwert und Unabhängigkeit hinsichtlich des Preises und Kapazität bieten (vgl. Cummins et al. 2009, S. 493 ff.). Allerdings ist zu beachten, dass in Zukunft nicht von diesem wechselnden Zeichnungsverhalten ausgegangen wird. Es wird vielmehr erwartet, dass dauerhaft ein weicher Markt vorliegt, welcher sich aufgrund geografischer Schadenereignisse allenfalls regional verhärteten kann.

Insbesondere der technische Fortschritt in verschiedenen Modellierungstechniken hat es ermöglicht, die Sammlung, die Analyse und die Auswertung von Daten zu verbessern und zu erleichtern. Durch die gesammelten Daten können detailliert Katastrophen oder andere Ereignisse modelliert werden. Dies gestattet potenziellen Investoren eine deutlich gesteigerte Transparenz des Versicherungsmarktes sowie des eingegangenen Risikos. Dadurch ergibt sich für Investoren eine attraktive und transparente Investitionsmöglichkeit (vgl. Cummins et al. 2009, S. 494).

Begünstigend für den Alternativen Risikotransfer war ebenfalls die Finanzkrise 2008–2009. Obwohl insbesondere Anfang 2008 aus Angst vor den Auswirkungen der Finanzkrise viel Kapital aus dem Markt für Alternativen Risikotransfer abgezogen wurde, konnte der Markt für Insurance-Linked-Securities (ILS) in dieser Zeit seine Krisenfestigkeit beweisen. Während der S&P Index 2008 ungefähr 34,5 Prozent verlor und im Jahr 2009 ca. 35 Prozent zulegte, hat der ILS-Sektor mit Renditen von 3,92 Prozent und 9,11 Prozent (laut dem Eureka ILS Index) überzeugende und stabile Renditen erzeugt. Dies führte dazu, dass das Vertrauen der Investoren in den ILS-Markt gestärkt wurde.

19.3 Kapitalmarktprodukte

Der Bereich Kapitalmarktprodukte konzentriert sich auf Instrumente, die versicherungs-technisches Risiko mithilfe originärer oder derivativer Finanztitel direkt auf den Kapitalmarkt übertragen. Die beiden am meisten verbreiteten Instrumente dieser Ausprägung sind Insurance-Linked-Securities (auch Insurance-Linked-Bonds) und derivative Kapitalmarktinstrumente mit versicherungstechnischem Underlying (vgl. Liebwein 2018, S. 476). Der Begriff Insured-Linked-Securities schließt, im Gegensatz zu Insured-Linked-Bonds, ebenfalls Derivate mit versicherungstechnischem Underlying ein.

Der Vorgang der Verbriefung der Versicherungsrisiken am Kapitalmarkt wird als Securitization bezeichnet. Hierbei wird zwischen der primären und sekundären Securitization unterschieden. Bei der primären Securitization transferieren Erst- oder Rückversicherungsunternehmen verbrieftete Risiken über den Kapitalmarkt direkt auf die Investoren. Im Gegensatz zur primären Securitization wird bei der sekundären Securitization ein Unternehmen als Vermittler zwischen Erst- und Rückversicherer und Kapitalmarkt geschaltet (vgl. Schwepcke et al. 2017, S. 147).

Um die Funktionsweise von Insurance-Linked-Bonds/-Securities und derivativen Kapitalmarktinstrumenten mit versicherungstechnischem Underlying darzustellen, werden im folgenden Cat-Bonds (Insurance-Linked-Bonds/-Securities) und Wetter- und Katastrophen-derivate sowie Katastrophen-Swaps (Derivate mit versicherungstechnischem Underlying) dargestellt.

19.3.1 Cat Bonds

19.3.1.1 Definition Cat-Bonds

Catastrophe-Bonds (kurz: Cat-Bonds), auch Katastrophenanleihen oder Katastrophenbonds genannt, sind die bekannteste und am weitesten verbreitete Art von Insurance-Linked-Bonds/-Securities (ILB) zur Verbriefung von Risiken (vgl. Wagner 2008, S. 129).

Im Regelfall sind Cat-Bonds als couponzahlende Bonds ausgestaltet, deren Auszahlung an ein die Zahlung auslösendes Ereignis (Trigger Event) geknüpft ist (zum Beispiel an ein Erdbeben mit einer Mindeststärke von 8,5 auf der Richterskala). Die Investoren erhalten pro festgelegter, eventfreier Periode eine vorher vereinbarte Couponzahlung.

Sobald das als Trigger definierte Ereignis stattfindet, erhält der Sponsor (Zedent) das von den Investoren investierte Kapital je nach Schwere des Ereignisses, entweder in voller Höhe oder gestaffelt (vgl. Damnjanovic et al. 2010, S. 1754 f.).

19.3.1.2 Struktur eines Cat-Bonds

In der Struktur eines Insured-Linked-Bonds, hier eines Cat-Bonds, gibt es fünf verschiedene Parteien: den Sponsor, das Special Purpose Vehicle (SPV), den Investor, den Treuhänder und den Swap-Kontrahenten.

Bei dem Sponsor handelt es sich um die Partei, die ihr Risiko auf die Investoren transferieren will. Der Sponsor kann Erstversicherer, Rückversicherer, ein Unternehmen sowie der Staat sein (vgl. Damnjanovic et al. 2010, S. 1754 ff.).

Der Sponsor (oder ein kooperierender Rückversicherer als Partner) gründet ein eigens für diesen Zweck gestaltetes selbstständiges Unternehmen, ein sogenanntes „Special Purpose Vehicle“ (SPV). Dieses Unternehmen besitzt entweder eine eigene Rückversicherungslizenz oder schließt einen Rückversicherungsvertrag mit dem kooperierenden Rückversicherer ab. Das gewählte Portfolio oder die einzelnen Risiken werden von dem Sponsor per traditionellem Rückversicherungsvertrag an das SPV zediert.

Nachdem die Risiken auf das SPV übertragen wurden, nimmt das SPV die Emission der ILB vor und ermöglicht so, dass Investoren in das versicherungstechnische Risiko des Bonds investieren. Anschließend ist die hauptsächliche Aufgabe des Special Purpose Vehicle, das Kapital der Investoren zur Deckung des versicherungstechnischen Risikos des Sponsors zu verwalten. Es muss garantiert werden, dass das Kapital zum Zeitpunkt eines auslösenden Ereignisses zur Verfügung steht. Um dies zu gewährleisten, wird das Kapital durch Wertpapiere und Staatspapiere mit hoher Bonität refinanziert (vgl. Liebwein 2018, S. 507). Eine weitere Funktion des SPV ist es, dem Sponsor eine bilanzielle Anerkennung der Transaktion als Rückversicherung zu ermöglichen und außerdem dem Investor zu garantieren, dass das investierte Kapital zweckgebunden verwendet wird. In einer primären Securitization hingegen wäre das investierte Kapital zusätzlich durch das komplette versicherungstechnische sowie unternehmerische Risikos des Versicherers gefährdet. Die Gründung des SPV erfolgt aus steuerlichen und regulatorischen Gründen gewöhnlich auf einem Offshore-Finanzplatz als Rückversicherungsunternehmen, wie zum Beispiel auf den Cayman Islands (vgl. Eickstädt 2001, S. 183 f.).

Der angebotene Zins für die Investoren setzt sich aus zwei Teilen zusammen: der Basisverzinsung und der Zusatzrendite. Die Basisverzinsung ergibt sich im Regelfall aus der Verzinsung der Staatspapiere bzw. der Wertpapiere mit hoher Bonität oder einem vereinbarten Referenzzinssatz (zum Beispiel dem 3-Monats-Libor). Zusätzlich zum Basiszinssatz erhalten die Investoren eine versicherungstechnische, risikoabhängige Zusatzrendite. Durch die Swap-Counterparty wird ermöglicht, die festgelegten Zinsen der Staatspapiere gegen die variablen Zinsen des Referenzzinssatzes zu tauschen. Dadurch kann sichergestellt werden, dass den Investoren ihr vereinbarter Basiszinssatz zu den vereinbarten Terminen ausgezahlt werden kann (vgl. Liebwein 2018, S. 507 f.).

Zusätzlich zu den genannten Parteien werden teilweise noch externe Unternehmen zur Risikomodellierung und Bewertung der Bonität der Emission beauftragt. Diese Daten werden genutzt, um eine angemessene Zusatzrendite zu ermitteln. Durch die Vergabe an externe Unternehmen werden moralische Risiken vermieden und eine Unabhängigkeit der Ergebnisse gewährleistet. Der gesamte Prozess der Platzierung, nachdem die Zielsetzung des ILB festgelegt wurde, beträgt üblicherweise sechs bis zwölf Monate (vgl. Liebwein 2018, S. 508).

19.3.1.3 Trigger-Arten

Bei Insurance-Linked-Securities kommt der Auswahl des auslösenden versicherungstechnischen Risikoereignisses (Trigger) eine zentrale Bedeutung zu. Nachfolgend werden die in der Praxis wesentlichen Trigger-Arten vorgestellt: der parametrische Trigger (Pure Parametric Trigger), der parametrische Index-Trigger, der Markt- oder Industrieschaden-Trigger (Industry Index Trigger) und der Modellschaden-Trigger (Modelled Loss Trigger)

Parametrischer Trigger

Bei den parametrischen Triggern (auch Pure Parametric Trigger oder physikalischer Trigger; vgl. Nguyen 2007, S. 258) werden die Schadenzahlungen durch ein physikalisch messbares Ereignis ausgelöst, wie zum Beispiel durch ein Erdbeben mit einer bestimmten Stärke auf der Richterskala. Die Deckung hängt davon ab, ob das definierte Ereignis in der definierten Form eingetreten ist und nicht, ob der zierten Partei tatsächlich Schäden entstanden sind (vgl. Wagner 2008, S. 455). Die Transparenz, ob das definierte Ereignis eingetreten ist, ist sehr hoch, da die Messdaten von verschiedenen unabhängigen Unternehmen dokumentiert werden und somit einer objektiven Überprüfung standhalten müssen. Zu beachten ist allerdings, dass der Trigger sich nicht auf die entstandenen Schäden bezieht. Somit muss die Entschädigung aus der Insurance-Linked-Security nicht deckungsgleich zu den tatsächlichen Schäden des Versicherers sein. Dadurch kann eine erhebliche Abweichung zwischen Schadenhöhe und Schadenzahlung verursacht werden (vgl. Liebwein 2009, S. 471). Da die erwarteten Verluste unabhängig von dem Verhalten der Vertragspartner sind und in diesem Fall keiner der Vertragspartner Einfluss auf das Versicherungereignis hat, kann Moral Hazard bei dieser Triggerart ausgeschlossen werden. Gleiches gilt für die Gefahr der adversen Selektion, da für den parametrischen Trigger historische Daten des entsprechenden Ereignisses zur Bewertung einer Insurance-Linked-Security entscheidend sind und der Emittent aus diesem Grund keine Möglichkeit hat, zwischen guten und schlechten Risiken zu selektieren. Für den Emittenten kann allerdings ein hohes Basisrisiko bestehen, da nicht zwingend eine hohe positive Korrelation zwischen den vom Emittenten zu zahlenden Entschädigungsleistungen und dem parametrischen Trigger besteht (vgl. Liebwein 2009, S. 264).

Branchenindextrigger

Bei Branchenindex-Triggern (Industry Index Trigger) ist die Bemessungsgrundlage des branchenweiten bzw. marktweiten Gesamtschadens aufgrund eines vereinbarten Versicherungereignisses. Wird der Trigger aktiviert, erhält das emittierende Unternehmen einen Prozentsatz der entstandenen Branchenschäden innerhalb der vereinbarten Mindest- und Höchstentschädigungsgrenzen (vgl. Nguyen 2007, S. 260 f.). Die Transparenz nimmt für den Investor aufgrund der zeitlichen Diskrepanz zwischen Schadeneintritt und Schadeneinstellung ab. Dies liegt vor allem daran, dass erst die Daten für die Erstellung des Index gesammelt werden müssen (vgl. Liebwein 2009, S. 471). Allerdings kann der Investor historische Versicherungsschadenverläufe analysieren, um einen groben Erwartungswert zu ermitteln, ohne das individuelle Portfolio des Emittenten zu kennen. Zusätzlich ist auf-

grund der geringen Möglichkeit der Einflussnahme des Emittenten auf den ermittelten Index das Risiko von Moral Hazard und adverser Selektion als gering einzuschätzen (vgl. Nguyen 2007, S. 261 f.). Zu beachten ist außerdem, dass der Absicherungsgrad für Unternehmen davon abhängt, wie sehr das entsprechende Portfolio dem Marktdurchschnitt folgt (vgl. Liebwein 2009, S. 471), und daraus ein Basisrisiko für den Emittenten entstehen kann, wenn die Unternehmensschäden nicht vollständig mit den Branchenschäden korrelieren (vgl. Nguyen 2007, S. 261).

Modellschadentrigger

Bei Modellschaden-Triggern (Modelled Loss Trigger) werden Schätzungen von Schadefrequenz und -höhe verwendet, die durch externe Modelle ermittelt werden (vgl. Nguyen 2007, S. 261). Diese Modelle werden zur hypothetischen Schadeneinschätzung eines Ereignisses auf ein Zielportfolio angewendet. Die verwendeten Daten bestehen einerseits aus definierten Portfolio-Informationen und andererseits aus physischen Messwerten (vgl. Liebwein 2009, S. 471). Besonders zu beachten ist, dass die errechnete Auszahlung nicht auf den tatsächlich aufgetretenen Schäden basiert, sondern auf den theoretisch errechneten Schäden. Dadurch entsteht ein mögliches Basisrisiko für den Emittenten, wenn der modellierte Schaden nicht dem tatsächlichen Schaden entspricht (vgl. Nguyen 2007, S. 262). Für den Investor kann die Transparenz dabei höher sein als bei dem Branchenindextrigger. Dies gilt auch für die Absicherung des Erstversicherers. Dies hängt jedoch von dem Grad der Komplexität und der Passgenauigkeit des Modells ab (vgl. Liebwein 2009, S. 471). Aufgrund der hypothetischen Ermittlung der Schadenzahlung kann bei dieser Art des Triggers Moral Hazard und Adverse Selektion ausgeschlossen werden (vgl. Nguyen 2007, S. 263).

Entschädigungsbasierter Trigger

Der entschädigungsbasierte Trigger (Indemnity Trigger) basiert auf dem tatsächlichen Schadenverlauf eines Versicherers und wird aktiviert, sobald eine entsprechende Schadenbelastung überschritten wird. Es besteht somit ein direkter Zusammenhang zwischen dem entstandenen Versicherungsschaden und der vereinbarten Zahlung. Der Vorteil dieser Form des Triggers für das emittierende Unternehmen ist, dass kein Basisrisiko besteht. Die Gefahr der Abweichung der Entschädigungsleistung vom tatsächlich entstandenen Schaden ist somit nicht gegeben. Dieser Vorteil gestaltet sich für die Investoren jedoch als Nachteil, da die Gefahr besteht, dass der Emittent bewusst höhere Schäden angibt, um die Rückzahlung an die Investoren zu kürzen. Aufgrund der Gefahr des Moral Hazard und adverser Selektion muss der Emittent im Regelfall einen erhöhten Risikozuschlag anbieten (vgl. Nguyen 2007, S. 258 f.). Insgesamt sind die entschädigungsbasierten Trigger vergleichbar mit klassischen Rückversicherungsverträgen. Deswegen ist die gebotene Transparenz für Investoren hier als eher gering einzuschätzen (vgl. Liebwein 2009, S. 471).

Parametrischer Index-Trigger

Bei dem parametrischen Index-Trigger handelt es sich um eine Weiterentwicklung des parametrischen Triggers, bei welchem das Raster der parametrischen Datensammlung verfeinert, unternehmensindividuell gewichtet und zu einem Gesamtindex zusammengefasst wird (vgl. Liebwein 2009, S. 471). Durch diese Maßnahmen wird versucht, eine Bezugsgröße zu schaffen, welche für den Emittenten das Basisrisiko verringert und für die Investoren das Risiko von adverser Selektion und Moral Hazard ausschließt. Bei indexbasierten Trigger-Arten ist es schwierig, das Basisrisiko für den Emittenten vollständig auszuschließen, da generell die Gefahr besteht, dass der unternehmensindividuelle Schaden nicht dem durch den Index ermittelten Schaden entspricht. Jedoch ist das Basisrisiko durch die unternehmensindividuelle Gewichtung deutlich geringer als bei dem reinen parametrischen Trigger (vgl. Nguyen 2007, S. 265 ff.). Für die Investoren bedeutet der parametrische Index-Trigger eine hohe Transparenz. Für die Passgenauigkeit zum Portfolio des Versicherers besteht allerdings Verbesserungspotenzial im Vergleich zu entschädigungsisierten Triggern (vgl. Liebwein 2009, S. 471).

19.3.2 Wetter und Katastrophenderivate

Derivate sind Finanzinstrumente, deren Wert sich nach den Wertentwicklungen von zugrunde liegenden Variablen richtet. Wetter- und Katastrophenderivate fallen unter den Begriff der Versicherungsderivate. Bei diesen hängt der Wert an der Entwicklung der auftretenden Versicherungsschäden (sogenanntes versicherungstechnisches Underlying) (vgl. Laudage 2009, S. 33). Versicherungsderivate stellen Kapital erst nach Schadeneintritt zu Verfügung. Grundlage für die Auszahlung sind im Regelfall Marktschadenindizes (vgl. Wagner 2008, S. 711).

19.3.2.1 Wetterderivate

Bei Wetterderivaten handelt es sich, historisch gesehen, um relativ neue derivative Finanzinstrumente, welche durch die globalen Wetterschwankungen in den letzten 15 bis 20 Jahren eine rasante Entwicklung genommen haben. Sie können sowohl zur Absicherung von wetterbedingten Schadenrisiken als auch zur reinen Spekulation verwendet werden. Unternehmen können sich mit Wetterderivaten gegen schwankende Temperaturen absichern, wenn diese Auswirkungen auf den wirtschaftlichen Ertrag des Unternehmens haben. Ein Beispiel ist der reduzierte Stromverbrauch in einem milden Winter bei einem Stromerzeugungsunternehmen (vgl. Riedler et al. 2013, S. 11). Bei den populärsten Wetterderivaten, beim Handel schwerpunktmaßig Optionen, sind die Grundlagen zur Auszahlung Heating-Degree-Days (HDD) oder Cooling-Degree-Days (CDD). Diese sehen Entschädigungszahlungen vor, basierend auf der Anzahl von Tagen in einem vereinbarten Zeitraum, in dem die Temperatur unter bzw. über einem festgelegten Wert liegt. Die Festlegung als HDD oder CDD erfolgt aus der Differenzrechnung (absolute Zahlen) zwischen einer festgelegten Referenztemperatur und der tatsächlichen Durchschnittstemperatur. Ist

die tatsächliche durchschnittliche Temperatur größer als die Referenztemperatur, handelt es sich um einen HDD. Ist die tatsächliche Durchschnittstemperatur tiefer, handelt es sich um einen CDD.

Während HDDs im Regelfall die Durchschnittstemperatur im Winter messen, messen CDDs im Regelfall die Durchschnittstemperatur im Sommer. Somit ist es zum Beispiel möglich, sich mit CDD Optionen gegen zu kalte Sommer und mit HDD Optionen gegen zu warme Winter abzusichern.

Es wird eine Proportionalitätskonstante (Tick) gebildet, die festlegt, wie stark sich die Auszahlungssumme pro Indexeinheit (hier Degree Days) verändert. Die Höhe der Auszahlung (Tick Size) wird per Tick festgelegt. Ab einer bestimmten Anzahl von Degree Days kann die Option ausgeübt werden (Strike Value). Zu beachten ist, dass zur Erzielung eines positiven Resultats aus der Option bei einem Call der Strike Value unter der Summe und bei einem Put der Strike Value über der Summe der tatsächlichen Degree Days liegen muss (vgl. Müller et al. 2000, S. 1 ff.) (Tab. 19.1).

Angenommen, ein in Köln tätiger Energieversorger möchte sich gegen mangelnde Stromnachfrage aufgrund eines kalten Sommers und den daraus resultierenden Umsatzverlust (aufgrund geringer Nutzung von Klimaanlagen) absichern, könnte dies wie in Tab. 19.2 gestaltet sein.

In diesem Beispiel beträgt der Strike Value 522,94 °C. Dies würde einer Durchschnittstemperatur (hier im Zeitraum von 180 Tagen) von 22,24 °C entsprechen. Sofern diese erreicht ist, kann die Option gezogen werden (vgl. Müller et al. 2000, S. 6).

Neben den Temperaturen können auch einzelne Ereignisse, wie zum Beispiel Schneehöhen oder Niederschlagsmengen, als Messgröße vereinbart werden (vgl. Eickstädt 2001, S. 171). Vorteile von Wetterderivaten sind insbesondere die hohe Transparenz sowie ein hoher Grad an Standardisierung, die auch den Handel von kleineren Transaktionen wirtschaftlich machen können. Die Nachteile von Wetterderivaten sind zum einen ein hohes Basisrisiko aufgrund des parametrischen Triggers (vgl. Cummins et al. 2009, S. 38) sowie ein fehlendes einheitliches Bewertungsverfahren. Dies kann Probleme bei der Einigung von Marktteilnehmern und eine hemmende Partizipation verursachen (vgl. Riedler et al. 2013, S. 20).

19.3.2.2 Katastrophen-Futures und -Options

Aufgrund des hohen Schadenumfangs von Hurrikan „Andrew“ im Jahr 1992 wurde die Kapazität des Erst- und Rückversicherungsmarktes infrage gestellt und nach alternativen Absicherungen für Katastrophen gesucht. Bereits 1992 wurden die ersten Katastrophen-

Tab. 19.1 Systematik bei Wetter-Optionen mit Referenztemperatur (vgl. Müller et al. 2000, S. 5)

Optionstyp	Absicherung gegen:	Ausübung bei	Auszahlungsbetrag
CDD Call	zu warmer Sommer	CDD>Strike Value	Tick Size(CDD-Strike Value)
CDD Put	zu kalter Sommer	CDD<Strike Value	Tick Size(Strike Value-CDD)
HDD Call	zu kalter Winter	HDD>Strike Value	Tick Size(HDD-Strike Value)
HDD Put	zu warmer Winter	HDD<Strike	Tick Size(Strike Value-HDD)

Tab. 19.2 Beispielhafte vereinfachte Wetteroption (orientiert an Müller et al. 2000, S. 6)

Stadt	Beginn	Ende	Optionsart	Strike Value* (°C.)	Tick Size (Euro)	Preis (Euro)	Ref. Temp. (°C.)
Köln	01.05.2018	31.10.2018	CDD Put	522,94	13.350	298.150	18,33

*gemessen in CDD

Futures und -Options auf dem Finanzmarkt vorgestellt. Aufgrund der geringen Nachfrage wurden diese jedoch schon im Jahr 2000 vom Markt genommen. Die Ursachen hierfür waren zum Beispiel fehlende Expertisen der Versicherer im Handel von Optionen und ein zu hohes Basisrisiko. Auch spätere Versuche zur Etablierung scheiterten (vgl. Cummins et al. 2009, S. 516 ff.). Bei Futures verpflichten sich die beteiligten Parteien, zu einem definierten Termin in der Zukunft ein vereinbartes Gut zu einem vorher verhandelten Preis zu kaufen (sogenannte Long-Position) oder zu verkaufen (sogenannte Short-Position). Bei Katastrophen-Futures ist das Underlying, also die verknüpfte zugrunde liegende Variable, ein versicherungstechnisch determinierter Schadenindex (vgl. Laudage 2009, S. 34 f.). Bei Katastrophen-Options handelt es sich um bedingte Termingeschäfte, bei denen das Underlying ebenfalls versicherungstechnisch determiniert ist. Bei bedingten Termingeschäften kann eine der Vertragsparteien wählen, ob das Geschäft zu einem vereinbarten Zeitpunkt (sogenannte europäische Option) oder jederzeit (sogenannte amerikanische Option) durchgeführt werden soll. Die Vertragspartei mit dem Wahlrecht kann entweder die Kaufoption (sogenannte Put-Option) oder Kaufoption (sogenannte Call-Option) haben (vgl. Ben Ammar et al. 2015, S. 36).

Die Vorteile von Katastrophen-Futures und Options sind eine hohe Standardisierung und eine schnelle Ausführung des Handels. Die Nachteile sind ein hohes Basisrisiko durch die Bindung an einen Marktschadenindex sowie fehlende vorteilhafte steuerliche und regulatorische Regelungen durch mangelnde Akzeptanz der entsprechenden Institutionen (vgl. Ben Ammar et al. 2015, S. 36). Ein weiteres Problem ist die Suche nach einem passenden Vertragspartner für den Versicherer. Der Versicherer muss eine Gegenpartei finden, die von einer Katastrophe profitiert oder auf diese spekuliert. Die Gruppe dieser Parteien ist relativ beschränkt. So können dies zum Beispiel Unternehmen aus der Baubranche sein, die aufgrund einer erhöhten Auftragslage nach einer Katastrophe profitieren. Hinzu kommt, dass ein Markt für Termingeschäfte nur dann effizient arbeiten kann, wenn genügend Liquidität vorhanden ist und dieses den Investoren ermöglicht, ihre Positionen flexibel zu ändern. Dies mindert die Aktivität der Investoren in diesem Bereich, da dies im Handel mit Versicherungsderivaten nicht der Fall ist (vgl. Flämig 2007, S. 143 ff.).

19.3.2.3 Katastrophen-Swaps

Katastrophen-Swaps sind eine weitere Art von Versicherungsderivaten. Bei einer Katastrophen-Swap-Transaktion zahlt der Versicherer (Zedent) periodisch Prämien im Austausch für eine festgelegte oder (je nach Schwere des Schadens) variable Zahlung durch eine andere Partei bei einem Trigger-auslösenden Event. Da die Katastrophen-Swaps außerbörslich gehandelt werden, können die Konditionen für den Swap entweder direkt

mit der anderen Partei oder durch einen Vermittler auf dem Finanzmarkt vereinbart werden. Neben dem Vertragszeitraum und dem definierten Event ist die Benennung eines definierten Referenzschadens für die Aktivierung des Swaps besonders wichtig. Dies geschieht meistens mithilfe eines Schadenindexes. Berücksichtigt wird dabei der Schaden, der durch das definierte Event in einer bestimmten Region verursacht wird. Tritt ein entsprechendes Ereignis auf und verursacht die vereinbarte Schadenhöhe, greift der Swap (vgl. Riedler et al. 2013, S. 32 ff.).

Katastrophen-Swaps haben den Vorteil, dass sie im Vergleich zu anderen Instrumenten einfach auszuführen sind, geringe fixe Kosten haben und keine Kapitalbindung an einen bestimmten Rückversicherer haben. Ein Nachteil ist allerdings, dass sie nicht voll besichert sind und somit ein Kreditrisiko für den Käufer besteht (vgl. Cummins et al. 2009, S. 521).

19.3.2.4 Versicherungstechnische Swaps

Möglich ist außerdem, dass zwei (Rück-)Versicherer verschiedene Blöcke ihrer Portfolios gegeneinander austauschen, um ihr vorhandenes Risiko im eigenen Portfolio zu diversifizieren (vgl. Cummins et al. 2009, S. 520). Bei diesem Tausch zwischen (Rück-)Versicherern handelt es sich, genauer definiert, um einen Austausch von Zahlungsströmen, das heißt der eingehenden Beitragseinnahmen und der (zukünftig) regulierten Schadenzahlungen der jeweiligen Portfolios. Durch die Reduzierung auf die Zahlungsströme eines Portfolios ist es möglich, auch nur bestimmte Teilkollektive des Portfolios zu tauschen (zum Beispiel anhand der versicherten Gefahr, regionaler Merkmale oder des Versicherungszweiges).

Ein theoretisches Beispiel für einen versicherungstechnischen Swap ist die Vereinbarung zweier Versicherer aus verschiedenen Ländern, die Hälfte ihres gezeichneten Sachversicherungsgeschäftes miteinander zu tauschen (zum Beispiel die entsprechenden Zahlungsströme) (vgl. Liebwein 2018, S. 522).

19.4 Rückversicherungsprodukte: Strukturierte Rückversicherung

Bei strukturierter Rückversicherung handelt es sich um Rückversicherungslösungen, die nicht als primäres Ziel den Risikotransfer verfolgen, sondern zu einem größeren Anteil andere Zielsetzungen verfolgen. Diese Zielsetzungen können finanzielle und ergebniswirtschaftliche Effekte, risikopolitische Effekte (bezogen auf das versicherungstechnische Risiko) sowie Effekte in der Kapital- und Risikosteuerung sein. Das primäre Ziel strukturierter Rückversicherung ist somit die Einflussnahme auf die gesamtunternehmerische Steuerung und nicht der versicherungstechnische Risikotransfer. Im Regelfall sollen durch den Transfer versicherungstechnischer Risiken auch weitere positive Effekte erzielt werden, es kommt also auf die Gewichtung der jeweiligen Zielsetzung an (vgl. Liebwein 2018, S. 377).

Es lässt sich festhalten, dass sich strukturierte Rückversicherungsverträge in der Struktur nicht grundsätzlich von klassischen Rückversicherungsverträgen unterscheiden. Allerdings werden zusätzliche Faktoren, wie erzielte Kapitalerträge, eine erhebliche Ergebnisteilung und eine limitierte Haftung des Zessionars, berücksichtigt. Durch diese Elemente in den Verträgen erfolgt der Risikotransfer nur bedingt.

Im Gegensatz zur Mehrheit der Instrumente des ART, die sich aufgrund der hohen Kosten sowie der limitierten Kapazitäten des traditionellen Versicherungsmarktes gegründet haben, legt strukturierte Rückversicherung den Fokus auf Bilanzpolitik. Der Faktor des Risikotransfers ist oft nur aus aufsichtsrechtlichen Gründen in das Instrument integriert. Bilanziell berücksichtigt wird dies zum Beispiel durch die Diskontierung von Schadenreserven oder die Verteilung einer finanziellen Belastung aufgrund eines Schadenfalles auf mehrere Jahre. Es kann jedoch auch Produkte geben, die eine Versicherung von Risiken ermöglichen, die auf dem traditionellen Versicherungsmarkt nicht vorhanden ist.

Im Zusammenhang mit strukturierter Rückversicherung wird oft auch der Begriff „Finite Reinsurance“ oder Finanzrückversicherung verwendet. Hier ist jedoch eine allgemeingültige Definition schwierig zu formulieren, da verwendete Begriffe häufig durch das verwendende Unternehmen definiert werden. Es handelt sich jedenfalls bei der Finanzrückversicherung insgesamt um ein Teilgebiet der strukturierten Rückversicherung.

Da der jeweilige Einsatzbereich von Rückversicherung sehr individuell und die Zielsetzung der verschiedenen Methoden unterschiedlich ist, steht klassische Rückversicherung nicht unbedingt in Konkurrenz zu strukturierter Rückversicherung. Vielmehr ergänzen sich die verschiedenen Lösungen und gehen teilweise ineinander über (vgl. Liebwein 2018, S. 381).

Die Hauptunterteilung in strukturierter Rückversicherung erfolgt, unter Berücksichtigung auf welches Geschäft sich die Finanzrückversicherung bezieht, in retrospektive und prospektive Vertragsformen (vgl. Eickstädt 2001, S. 149).

19.4.1 Retrospektive Vertragsformen

Retrospektive Vertragsformen beziehen sich auf ein bereits abgeschlossenes Geschäft, in dem Schäden schon bekannt, noch unbekannt oder noch nicht bezahlt sind. Durch Diskontierung von Schadenreserven wird eine vorzeitige Realisation versicherungstechnischer Rückstellungen für noch nicht vollständig abgewickelte Schadenfälle erzielt. Dadurch kann im Jahr des Vertragsabschlusses eine Verbesserung des Betriebsergebnisses und des Eigenkapitals erreicht werden. Die retrospektiven Vertragsformen spielen in der Versicherungsbranche heutzutage nur noch eine untergeordnete Rolle (vgl. Eickstädt 2001, S. 149 ff.). Im Folgenden werden beispielhaft die beiden retrospektiven Vertragsformen des Loss-Portfolio-Transfers sowie des Adverse-Development-Covers vorgestellt.

19.4.1.1 Loss-Portfolio-Transfer (LPT)

Ein Loss Portfolio-Transfer (LPT) beschreibt die Übertragung eines Portfolios von Schadenzahlungsverpflichtungen von einem Erstversicherer auf einen Rückversicherer. Der Rückversicherer erhält im Gegenzug eine Einmalprämie. Die Prämie berücksichtigt die Auszahlungsgeschwindigkeit sowie eventuelle Ausfallrisiken. Dies führt beim Erstversicherer zu einer Bilanzverkürzung und zu einem ausgewiesenen Abwicklungsgewinn, einem höheren Eigenkapital sowie einer verbesserten Ist-Solvabilität (vgl. Eickstädt 2001, S. 150 ff.). Dies resultiert aus der Tatsache, dass Schadenreserven nicht diskontierte Werte in der Bilanz des Verkäufers darstellen. Die übertragenen Werte der Reserven übersteigen den Wert der bezahlten Prämie, was zu einer Reduzierung der Haftung des Versicherers führt. Die Ausgestaltung der Verträge erfolgt, wie in der klassischen Rückversicherung, als Schadenexzedent- oder als Quotenrückversicherung. Das Besondere hierbei ist, dass nicht das gesamte versicherungstechnische Risiko kalkuliert werden muss, sondern hauptsächlich das Risiko der Schadennachreservierung sowie des tatsächlichen Zahlungszeitpunktes, da die Schäden des Portfolios bereits eingetreten sind.

Durch die Übertragung der Verpflichtungen auf den Rückversicherer, kann der Erstversicherer sich aus diesem Geschäftsfeld zurückziehen und das Risikokapital anderweitig einsetzen. Durch den LPT können außerdem versicherungstechnisch schwer einschätzbare Risiken transferiert, der Rückzug aus bestimmten Anfall- oder Zeichnungsjahren schneller vollzogen sowie eventuelle Fusionen oder Akquisitionen erleichtert werden (vgl. Liebwein 2018, S. 413).

19.4.1.2 Adverse-Development Cover (ADC)

Der Adverse-Development-Cover (ADC) stellt eine Ergänzung zum LPT dar. Der Fokus des ADC liegt, im Gegensatz zum LPT, nicht auf der tatsächlichen Transferierung eines Portfolios, sondern auf dem Schutz vor nicht ausreichender Reservierung der Schäden (vgl. Eickstädt 2001, S. 151 ff.). Deckung besteht für bereits eingetretene, aber noch nicht gemeldete Schäden (sogenannte IBNR-Schäden, incurred but not reported), wenn deren Schadenreserve noch nicht ausreichend ist oder noch nicht gebildet wurde sowie für IBNER-Schäden (Incurred but not enough reported), wenn die gebildeten Reserven nicht ausreichen, um die tatsächliche Schadenzahlung zu decken. Die Vertragsgestaltung verläuft ähnlich wie bei der klassischen Rückversicherung. Die am häufigsten angewendeten Formen sind die Jahresüberschaden-Rückversicherungen (Stop-Loss), Einzel- oder Kumulschadenexzedenten (vgl. Laudage 2009, S. 25).

19.4.2 Prospektive Vertragsformen

Prospektive Vertragsformen beziehen sich auf Schäden, die zum Zeitpunkt des Vertragsabschlusses noch nicht aufgetreten sind und sich auf laufendes bzw. zukünftiges Geschäft beziehen. Nachfolgend werden die Formen Financial-Quota-Share-Agreement, strukturierte Stop-Loss- und Spread-Loss-Verträge vorgestellt.

19.4.2.1 Financial-Quota-Share-Agreement

Ein Financial-Quota-Share-Agreement (FQSA) ist als Quotenrückversicherungsvertrag gestaltet, dem zusätzlich noch eine finanzwirtschaftliche Komponente hinzugefügt wurde. Die Grundstruktur eines FQSA ist, dass der Erstversicherer die Haftung für eine Quote eines Portfolios an den Rückversicherer überträgt. Dieser erhält als Gegenleistung eine entsprechende Prämie. Die finanzwirtschaftliche Komponente ist hierbei die veränderte Zahlweise der Rückversicherungsprovision. Bei einem FQSA zahlt der Rückversicherer dem Erstversicherer zu Beginn des Vertrages eine erhöhte Rückversicherungsprovision und in den folgenden Jahren eine entsprechend vermindernde Provision. Dies kann einen möglichen Verlustausweis, zum Beispiel aufgrund von hohen Abschlusskosten, verhindern, da die Provision den Verlust kompensiert (vgl. Laudage 2009, S. 25 f.). Dies kann für jüngere oder expandierende Versicherer eine Art Aufbauhilfe darstellen, da die Abschlusskosten von Verträgen einen hohen Kostenpunkt darstellen können. Dieser Kostenpunkt kann so durch den Rückversicherer vorfinanziert werden. Dies ist aufgrund der hohen Abschlussprovisionen insbesondere für den Bereich der Lebensversicherung interessant (vgl. Liebwein 2009, S. 387).

19.4.2.2 Jahresüberschadenexzedenten (Strukturierte Stop-Loss-Verträge)

Ein Jahresüberschadenexzedent (auch Stop-Loss genannt) stellt einen Schadenexzedenten dar, bei dem der vom Rückversicherer getragene Schaden den Jahresschadenaufwand darstellt, der über der Priorität (Selbstbehalt des Erstversicherers) liegt. Die Priorität des Erstversicherers sowie die Haftung des Rückversicherers werden in der Regel als Prozentpunkte der Schadenquote festgelegt, sie können aber auch in absoluten Beträgen vereinbart werden. Die maximale Haftung der Rückversicherung (Plafond) sowie die minimale Priorität des Versicherers werden jedoch in absoluten Zahlen festgelegt. Der Schaden stellt die Summe aller Einzelschäden innerhalb eines Jahres dar, wenn die Priorität überschritten wird.

Der Vertragszeitraum beträgt in der Regel ein Jahr bei traditionellen Stop-Loss-Verträgen bzw. drei bis fünf Jahre bei strukturierten Stop-Loss-Verträgen und ist meistens deckungsgleich mit den Geschäftsjahren des Erstversicherers.

Stop-Loss-Verträge werden hauptsächlich im Bereich schwankungsanfälliger Kumulschadenpotenziale vereinbart, wie zum Beispiel bei der Rückversicherung von Erdbeben- oder Sturmgefahren. Reine Stop-Loss-Verträge sind auf dem Rückversicherungsmarkt nicht sehr verbreitet, da nach Überschreitung der Priorität alle Schadenzahlungen zu Lasten des Rückversicherers gehen (bis zur Erreichung des Plafonds). Um zu erreichen, dass der Erstversicherer weiterhin die Schäden so gering wie möglich halten will, gibt es verschiedene Gestaltungen der Priorität, die in die Deckung eingebaut werden können (vgl. Schwilling 2018, S. 29). Ein Beispiel kann eine bestimmte Schadenspanne innerhalb der Haftungsstrecke des Rückversicherers sein, die der Erstversicherer selbst tragen muss. Das Ziel einer Stop-Loss-Deckung ist somit die Begrenzung des möglichen Verlustes des Erstversicherers.

Insgesamt haben Jahresüberschadenexzedenten den Vorteil, dass der Erstversicherer in besonders schadenbelasteten Jahren entlastet wird, unabhängig von der Art der hohen Schadenbelastung (Frequenz oder Schwere der Versicherungsfälle). Außerdem ist eine planbare Belastung durch die festgelegte Priorität vorhanden. Zusätzlich ist der administrative Aufwand einer Stop-Loss-Deckung relativ gering.

Die Schwierigkeit bei einer Stop-Loss-Deckung besteht darin, den möglichen Jahreshöchstschaden zu ermitteln, da (nach Erreichung des Plafonds) keine Rückversicherungsleistung mehr gezahlt wird. Zusätzlich sind die Verträge in der Regel so gestaltet, dass sich der Erstversicherer bei Überschreitung der Priorität bereits in einer Verlustsituation befindet, damit durch die Absicherung kein Gewinn erzielt werden kann. Das komplette unternehmerische Risiko des Erstversicherers soll nicht übernommen werden, insbesondere nicht bewusste strategische Entscheidungen des Erstversicherers (vgl. Abb. 19.2).

Strukturierte Stop-Loss-Verträge sind in der Praxis deutlich weiter verbreitet. Durch sie kann eine Stabilisation der Gewinne erreicht und der eigene Aufbau von Kapital des Erstversicherers abgesichert werden. Sie funktionieren ähnlich wie die klassischen Stop-Loss-Verträge, jedoch betragen die Vertragslaufzeiten mehrere Jahre. Durch die mehrjährige Laufzeit können zusätzliche Faktoren, wie zum Beispiel Zinserträge, berücksichtigt werden. Außerdem ist es möglich, die Belastung durch einen hohen Schadenfall auf mehrere Perioden zu verteilen und somit die Schadenquote in einem schadenbelasteten Jahr zu glätten. Als Grundlage kann sowohl das Geschäftsjahr, das Anfallsjahr oder das Zeichnungsjahr vereinbart werden.

Bei der Integration einer strukturierten Stop-Loss-Deckung in das Rückversicherungsprogramm eines Erstversicherers kann die Priorität in den berücksichtigten Versicherungssparten erhöht werden, wenn dafür ab einem bestimmten Eintrittspunkt (üblicherweise

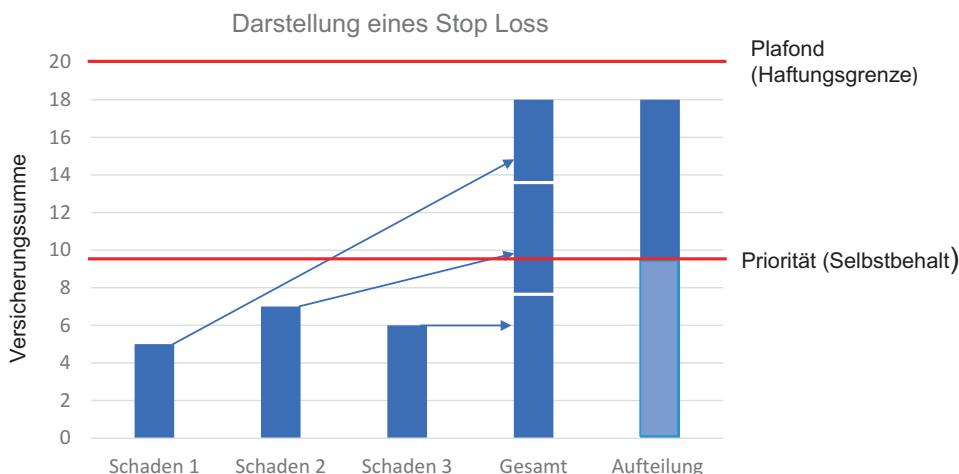
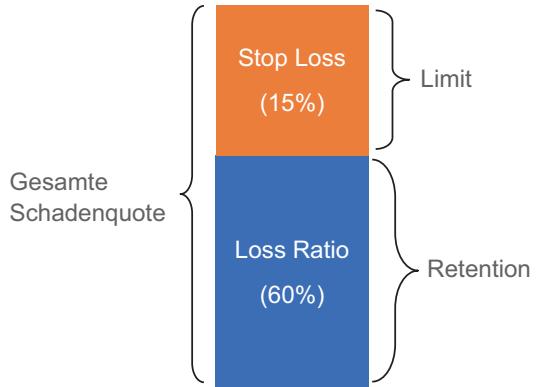


Abb. 19.2 Darstellung einer Stop-Loss Deckung. (Quelle: eigene Darstellung in Anlehnung an Gottwald 2015, S. 38)

Abb. 19.3 Beispiel der Reduzierung der Volatilität durch den Einsatz einer Stop-Loss Deckung. (Quelle: eigene Darstellung)



Schadenquote oder kombinierte Schaden- und Kostenquote) der Einsatz eines Stop-Loss-Vertrages vereinbart wird. Er kann folglich mit einer bestimmten Genauigkeit die Schätzung von Gewinnen, Überschüssen und der Schadenquote vornehmen. Durch den Einsatz der Stop-Loss-Deckung mit einer mehrjährigen Laufzeit wird die Volatilität des Nettoergebnisses reduziert und damit das Jahresergebnis stabilisiert (vgl. Abb. 19.3).

Der Jahresüberschadenexzedent kann mit verschiedenen Wirkungen zur Steuerung bilanzieller Kenngrößen eingesetzt werden. Wenn das primäre Ziel die Reduktion der Volatilität der bilanziellen Ergebnisse ist, ist die Berücksichtigung der Gewinn- und Verlustrechnung (GuV-Rechnung) sowie der HBG-Bilanz bei der Beurteilung der Rückversicherungsoptionen zu empfehlen. Zu beachten ist allerdings, dass die Bildung der Schadenreserven und der Schwankungsrückstellung der Erstversicherer einen glättenden Effekt auf die Bilanz haben und somit den notwendigen Bedarf an Rückversicherung für diesen Zweck reduzieren können. Möglich ist auch, durch einen mehrjährigen strukturierten Jahresüberschadenexzedenten, die Planbarkeit der Schwankungsrückstellung zu erhöhen.

19.4.2.3 Spread-Loss

Die Grundidee einer Spread-Loss-Deckung ist, dass es dem Erstversicherer ermöglicht wird, die finanzielle Belastung aufgrund eines schlechten Schadenverlaufes eines Vertragsjahrs durch die Aufteilung auf mehrere Vertragsjahre abzuschwächen. Er kann damit eine kontinuierliche und planbare Belastung sowie wenig Volatilität erreichen.

Die Struktur einer Spread-Loss-Deckung basiert auf einem nicht-proportionalen Rückversicherungsvertrag (Kumulschadenexzedent oder Einzelschadenexzedent), der durch ein Finanzierungsselement erweitert wird. Die zur Verfügung gestellte Haftung dieser Verträge wird in der Praxis teilweise vom Käufer finanziert und der verbleibende Rest dann durch Risikotransfer abgedeckt.

Für den Erstversicherer wird ein Erfahrungskonto eingerichtet, auf dem unter anderem die geleisteten Schadenzahlungen des Rückversicherers, die gezahlten Rückversicherungsprämien des Erstversicherers sowie ein entsprechender Saldo dieser Leistungen,

welches am Ende des Jahres gebildet wird, dokumentiert werden. Dieser Saldo wird im Regelfall erst am Ende der Vertragslaufzeit ausgeglichen. Hier ist auch eine prozentuale Ausgleichung des Saldos möglich, so kann zum Beispiel vereinbart werden, dass der Erstversicherer nur 50 Prozent des negativen Saldo ausgleicht oder dass der Rückversicherer 50 Prozent des positiven Saldo erhält (vgl. Liebwein 2018, S. 440 ff.). In der Praxis wird in der überwiegenden Anzahl der Fälle ein negativer Saldo (zu Lasten des Rückversicherers) gar nicht ausgeglichen. Das Erfahrungskonto und die üblicherweise mehrjährige Laufzeit von Spread-Loss-Deckungen ermöglichen es, dass in Jahren mit geringer Schadenbelastung die nicht verwendete Prämie (abzüglich der Risikoprämie für den Versicherer) des Erstversicherers dem Erfahrungskonto gutgeschrieben werden kann. Durch dieses Finanzierungselement kann in stark schadenbelasteten Jahren die vorher oder zukünftig generierte Gutschrift dazu verwendet werden, die Schadenlast abzuschwächen.

Die Verträge können vielfältig angepasst werden. So können beispielsweise auch Vereinbarungen getroffen werden, die den Erstversicherer bei einem negativen Saldo seinerseits im darauffolgenden Jahr zur Zahlung einer zusätzlichen Prämie verpflichten oder dem Erstversicherer eine besondere Kündigungsfrist bei einem guten Schadenverlauf zu gestehen (Abb. 19.4).

19.4.3 Contingent Capital

Bei Contingent Capital handelt es sich um verbriegte Transaktionen, die dem Versicherer oder Unternehmen erlauben, im Falle des Eintritts eines vorher definierten (rück-versicherungstechnischen Ereignisses (Trigger) in einem vorher bestimmten Zeitraum neue Aktien oder Anleihen zu einem vorher vereinbarten Preis zu emittieren (vgl. Cum-

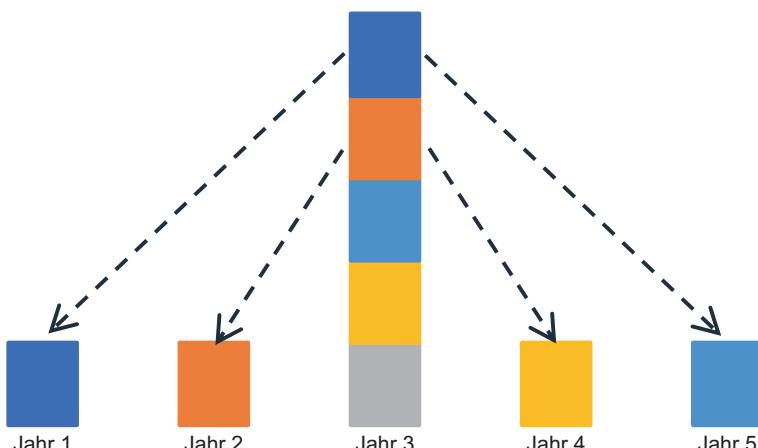


Abb. 19.4 Vereinfachte Darstellung der Idee einer Spread-Loss Deckung. (Quelle: eigene Darstellung)

mins et al. 2009, S. 516). Ziel ist es hierbei, in einer Liquiditätsknappheit die Bereitstellung von Kapital sowie eine gleichzeitige Reduzierung der Kapitalkosten zu gewährleisten. Die zwei am häufigsten verbreiteten Instrumente von Contingent Capital in der Versicherungsbranche sind Catastrophe Equity Puts (CEP) und Contingent Surplus Notes (CSN) (vgl. Eickstädt 2001, S. 87).

Die Catastrophe Equity Puts (CEP) ermöglichen es dem Versicherer, Aktien im Falle eines definierten Ereignisses zu einem vorher festgelegten Preis zu verkaufen. Es handelt sich also um eine Eigenkapitalzuführung. Die CEP sind auf die Auswirkung von Naturkatastrophen oder anderer definierter Katastrophen sowie auf den Verlust und die daraus resultierende Senkung der Aktienkurse des Unternehmens fokussiert. So muss (im Gegensatz zu normalen Put-Optionen) im Regelfall der Aktienpreis unter einen festgelegten Wert sinken und der aus der Katastrophe resultierende Verlust ein bestimmtes Schadenausmaß überschreiten (vgl. Kailan Shang 2013, S. 6).

Contingent Surplus Notes (CSN) stellen dem Unternehmen Genussscheinkapital und damit Fremdkapital zur Verfügung. Bei Transaktionen von CSN wird von einem SPV eine Wandelanleihe emittiert, durch die die Investoren dem SPV für eine bestimmte Laufzeit und gegen vereinbarte Zinsen einen bestimmten Kapitalbetrag zur Verfügung stellen. Sie erhalten im Gegenzug eine entsprechende Schuldverschreibung. Die Schuldverschreibung enthält die Klausel, dass bei Eintreten bestimmter versicherungstechnischer Determinanten die Schuldverschreibungen in Genussscheine an dem Versicherungsunternehmen hinter dem SPV umgewandelt werden. Somit wird für das Unternehmen bei Ereigniseintritt Fremdkapital bereitgestellt (vgl. Laudage 2009, S. 32 f.).

Durch die Erschließung externen Kapitals kann das Unternehmen kurzfristige Kapitalengpässe und so eine potenzielle Insolvenz vermeiden. Versicherer können sich so auch nach Eintritt von Naturkatastrophen mit Kapital versorgen (vgl. Eickstädt 2001, S. 86 f.).

Die Größe der Transaktion schwankt gewöhnlich zwischen einigen Millionen und einer halben Milliarde US-Dollar. Die Vorteile von Contingent Capital sind, dass keine Up-Front-Zahlung geleistet werden muss, die Finanzierung ohne weitere Zustimmung der Shareholder durchgeführt werden kann und die Bereitstellung von Kapital in den benötigten Situationen, wie dem Eintreten einer Katastrophe, erfolgt (vgl. Kailan Shang 2013, S. 6).

Bei Aktiengesellschaften sind die Nachteile von Contingent Capital hauptsächlich, dass durch die Emittierung von Aktien eine Schwächung der bestehenden Aktienhaberstruktur (der sogenannte Kapitalverwässerungseffekt) möglich ist, die bei Cat-Bonds oder Optionen nicht möglich wäre. Außerdem verändert das durch die Emission eingenommene Kapital die Kapitalstruktur des Unternehmens (vgl. Cummins et al. 2009, S. 516).

Zu berücksichtigen ist allerdings, dass Contingent-Capital-Lösungen hauptsächlich die Existenz eines Unternehmens nach einem Katastrophenereignis sicherstellen und keine Glättung der Resultate ermöglichen, da ein potenzieller Schaden voll in die Erfolgsrechnung einfließt. Ein großer Vorteil gegenüber klassischen Rückversicherungslösungen ist, dass bei Contingent-Capital-Lösungen eine langfristige Verfügbarkeit des Kapitals zu festgelegten Konditionen möglich ist, während Rückversicherungsprämien stark von der

zeitlich zuletzt eingetretenen Katastrophe beeinflusst werden (vgl. Eickstädt 2001, S. 89 ff.).

Ein Beispiel für eine Contingent Surplus Note Transaktion ist die 500 Millionen Euro Transaktion der Farmers Insurance Group im Jahr 2007: In diesem Fall hatte der Versicherer die Option verhandelt, dass im Falle eines Verlustes von mindestens 1,5 Milliarden US-Dollar aufgrund eines Windsturmes in den Gebieten Texas, Arkansas, Oklahoma oder Louisiana Schulscheine zu einem bestimmten Preis herausgegeben werden (vgl. Batten et al. 2012, S. 76).

19.5 Mischformen (hybride Instrumente)

Durch den historischen Wandel des Risikotransfermarktes haben sich darüber hinaus hybride Produkte entwickelt, die sowohl die Eigenschaften reiner Finanzinstrumente als auch Eigenschaften der klassischen Rückversicherung haben (vgl. Cummins et al. 2009, S. 501). Nachfolgend werden aufgrund ihrer hohen Relevanz die Produkte Collateralized Reinsurance, Sidecars und Industry Loss Warrenties vorgestellt.

19.5.1 Collateralized Reinsurance

Collateralized Reinsurance (CRe) bezeichnet privat strukturierte Vereinbarungen, welche ein bestimmtes Portfolio oder bestimmte Versicherungspolicen gegen ein vorher definiertes Ereignis absichern (vgl. Ben Ammar et al. 2015, S. 30 f.). Oft handelt es sich hierbei um einen traditionellen Rückversicherungsvertrag, der von einem Rückversicherer gefrontet und anschließend an einen Investor weitergegeben wird. Dieser Vorgang wird Collateralized Fronting genannt. Der Erstversicherer hat also einen traditionellen Rückversicherungsvertrag mit dem Rückversicherer. Er wird aber in der Regel darüber informiert, dass die erweitert Kapazität durch das Einbinden von Investoren ermöglicht wurde. Dies ist jedoch nicht zwingend der Fall.

Durch CRe können institutionelle Investoren, wie Hedgefonds oder Pensionsfonds, am Rückversicherungsmarkt aktiv werden und Risikokapital am Markt bereitstellen, um dadurch ihr Portfolio zu diversifizieren. Ein großer Unterschied zu der traditionellen Rückversicherung ist, dass das gesicherte Kapital im Voraus (Up-Front) zur Verfügung gestellt werden und dem Potenzial möglicher resultierender Schäden aus dem Rückversicherungsvertrag entsprechen muss. Die Laufzeiten der Verträge betragen im Regelfall ein Jahr. Die Verträge sind im Gegensatz zu Cat-Bonds nicht handelbar (vgl. Ben Ammar et al. 2015, S. 31 f.).

Vorteilhaft für Investoren ist die hohe Flexibilität in Bezug auf strukturtechnische Charakteristika und die zugrunde liegenden Risiken. Dies gibt den Investoren die Möglichkeit, ihre Portfolios gezielt weiter zu diversifizieren. Ein Nachteil ist die geminderte Liquidität, die durch die Vorauszahlung des Risikokapitals entsteht, sowie das asymmetrische Infor-

mationsverhältnis zwischen Käufer und Investor. Da CRe grundsätzlich entschädigungs-basiert ist, besteht für die Käufer kein Basisrisiko (vgl. Ben Ammar et al. 2015, S. 30 ff.).

19.5.2 Sidecars

Sidecars sind, ähnlich wie bei CRe, finanzielle Strukturen, die es Investoren ermöglichen, in ein bestimmtes Portfolio von Versicherungspolicen zu investieren. Sie sind im Regelfall voll besichert, das heißt, dass die potenziellen Schadensansprüche befriedigt werden können und die Investoren einen Ertrag auf das abgesicherte Portfolio erzielen (vgl. Liebwein 2009, S. 506 f.). Es handelt sich bei Sidecars um Rückversicherungsfirmen, die als Special Purpose Vehicle (SPV) strukturiert sind. Sie werden von einem Rückversiche-rungsunternehmen gegründet (einem sogenannten Sponsor) und ermöglichen institutio-nellen Investoren, wie zum Beispiel Hedgefonds, dem Unternehmen zusätzliche Kapital-kapazität bereitzustellen. Das von dem Sidecar gesammelte Kapital wird in einem Collateral Trust verwaltet, um das Kreditrisiko für den Sponsor zu reduzieren. Der Spon-sor vereinbart mit dem SPV einen Rückversicherungsvertrag, in dem vereinbart wird, dass der Sponsor eine Prämie für die gezeichneten Risiken zahlt und das SPV verpflichtet ist, die unter den Vertrag fallenden Schadenzahlungen zu ersetzen (vgl. Ben Ammar et al. 2015, S. 31 f.).

Im Gegensatz zu CRe wird das Kapital der Investoren bereits vor der Festlegung auf ein bestimmtes Portfolio eingezahlt, anstatt sich auf ein schon vorher spezifisches Portfolio zu konzentrieren. Die Aktivität von Sidecars erhöht sich besonders während einer „hard market“-Periode und reduziert sich im Laufe einer „soft market“-Periode. Insbesondere nach Hurrikan „Katrina“ im Jahr 2005 wurden Sidecars aufgrund der begrenzten und teuren Kapazität und der daraus resultierenden profitablen Margen für Investoren stark nachgefragt (vgl. Njegomir et al. 2009, S. 77). Die Risiken werden in der Regel über eine prozen-tuale Regelung an das SPV transferiert. Die transferierten Risiken können unter anderem aber auch Excess-of-Loss-Deckungen sein.

Ein Unterschied zwischen Sidecars und Cat-Bonds ist, dass der Erlös von Sidecars von den angemeldeten Schadenansprüchen abhängt und somit höher oder tiefer ausfallen kann, während Cat-Bonds fixe Couponzahlungen leisten (vgl. Ben Ammar et al. 2015, S. 31 f.). Ferner ermöglichen Cat-Bonds den Versicherern, ihre Katastrophenrisiken auf die Kapitalmärkte zu transferieren. Sidecars hingegen können jede Art gezeichneter Risiken der Versicherer auf den Kapitalmarkt übertragen. Die Struktur eines Cat-Bonds er-laubt, eine Vielzahl von Investoren einzubeziehen, während Sidecars in den meisten Fällen nur von vergleichsweise wenigen Investoren finanziert werden (vgl. Cummins et al. 2013, S. 569).

Im Regelfall werden Sidecars von Rückversicherern erstellt und anschließend Investo-ren angeboten. Dies ist der Grund dafür, warum Investoren Sidecars teilweise skeptisch sehen. Durch Selektion des Portfolios durch den Rückversicherer besteht ein potenzieller Interessenkonflikt zwischen Rückversicherer und Investor, da der Rückversicherer daran

interessiert sein könnte, besonders schadenträchtige Risiken aus seinem Portfolio heraus zu transferieren, um seine Risikostruktur zu glätten. Im Vergleich mit anderen Methoden des ART besitzen Sidecars eine hohe Kostenstruktur (vgl. Ben Ammar et al. 2015, S. 31).

Ein Vorteil von Sidecars ist, dass sie Investoren ermöglichen, in versicherungstechnische Risiken zu investieren, ohne zwangsläufig ein langfristiges Investitionsverhältnis einzugehen. Zusätzlich bieten Sidecars die Möglichkeit, leicht in den Markt ein- und auszutreten. Dies gibt Investoren die Chance, bei „hard market“-Phasen in den Markt einzutreten und bei dem Wechsel in eine „soft market“-Phase den Markt wieder zu verlassen. Ein weiterer Vorteil ist, dass Sidecars für Investoren, aufgrund der Ähnlichkeit zu traditionellen Investments in „equity“- und „debt-Securities, im Vergleich zu anderen Instrumenten des ART leichter zu verstehen sind (vgl. Njegomir et al. 2009, S. 77 ff.). Für Sponsoren ist vorteilhaft, dass im Gegensatz zur normalen Retrozession keine Underwritinginformationen oder andere Kalkulationsmethoden mit Konkurrenten geteilt werden müssen. Die Geschäftspartner bei einem Sidecar, wie zum Beispiel eine Bank oder ein Hedgefonds, sind im Regelfall nicht in der Versicherungsbranche aktiv (vgl. Cummins et al. 2013, S. 569)“.

19.5.3 Industry Loss Warrenties

Industry Loss Warrenties (ILW) sind ein weiteres Instrument der hybriden Kategorie zur Absicherung von Risiken. Ausgestaltet werden die ILW im Regelfall wie traditionelle Rückversicherungsverträge, um diese dann anschließend auch auf dem traditionellen Rückversicherungsmarkt zu platzieren.

Ähnlich wie bei Cat-Bonds verpflichtet sich der Verkäufer, den Käufer bei einem auslösenden Trigger Event zu entschädigen. Im Gegensatz zu Cat-Bonds sind ILW mit zwei Triggern ausgestattet. So kann die Gestaltung eines ILW beispielsweise mit einem Branchenindex-Trigger (Industry Index Trigger) in Kombination mit einem Schadentrigger (Indemnity Trigger) erfolgen. Im Regelfall ist der Branchenindex-Trigger deutlich höher als der Schadentrigger (vgl. Cummins et al. 2013, S. 547 ff.). Dabei wird der Schaden-Trigger im Regelfall sehr gering angesetzt, so dass die Wahrscheinlichkeit hoch ist, dass der Versicherer bei Aktivierung des Branchen-Triggers die Auszahlung erhält. Die Transparenz von ILW ist aufgrund der hohen Standardisierung bei Gestaltung und Ausformulierung der Verträge als hoch anzusehen. Die Deckungsspanne von ILW liegt zwischen einer Million und 250 Millionen US-Dollar. Die Vertragslaufzeit übersteigt in den wenigsten Fällen ein Jahr, jedoch steigt die Nachfrage nach mehrjährigen Verträgen, um langfristige Risiken abzusichern (vgl. Cummins et al. 2013, S. 566 f.). Ein weiterer Unterschied zu Cat-Bonds ist, dass der Investor das riskierte Kapital nicht zu Beginn des Vertrages hinterlegen muss, sondern erst, wenn die Zahlung durch die Trigger aktiviert wird. Diese Struktur verursacht allerdings ein Counterparty-Risiko, da die Nichtzahlung der vereinbarten Summe erst in dem Moment der Aktivierung des Triggers deutlich wird (vgl. Ben Ammar et al. 2015, S. 29). Die hohe Abhängigkeit der Auszahlung an den Branchenindex-Trigger verursacht ein Basisrisiko für den Käufer. Dieses kann durch eine individuellere Gestal-

tung des ILW vermindert werden (vgl. Cummins et al. 2013, S. 567). Jedoch kann die Situation eintreten, dass der Schaden-Trigger aktiviert wird, der Branchen-Trigger jedoch nicht und somit keine Auszahlung erfolgt. Dieses Basisrisiko ist höher für Unternehmen, deren Bedrohungen nicht dem Standard-Portfolio der Branche entsprechen. ILW werden also hauptsächlich von Unternehmen gekauft, deren Portfolio nah am Durchschnittsmarkt liegt, um hierdurch das Basisrisiko zu minimieren (vgl. Ali Ishaq 2005, S. 79).

Die zentrale Bedeutung des Branchenindex-Triggers bei der Auszahlungsermittlung hat den Vorteil, dass der Verkäufer im Regelfall keine Underwriting-Kenntnisse benötigt. Hauptsächlich muss also das Risiko der Aktivierung des Branchenindex-Triggers kalkuliert werden und nicht der eigentliche Verlust des Unternehmens (vgl. Cummins et al. 2013, S. 567).

Ein Beispiel (vgl. Tab. 19.3) für die Nutzung eines ILW ist, wenn ein Versicherer ein hohes Schadenzentral durch Hurrikane in Florida hat und dieses begrenzen will. Hier kann die Auszahlung durch einen ILW vereinbart werden, wenn durch einen Hurrikan ein industrieübergreifender Schaden in Höhe von 18 Milliarden US-Dollar und ein individueller Unternehmensschaden in Höhe von 15 Millionen US-Dollar verursacht wird.

19.6 Fazit und Ausblick

Alternativer Risikotransfer hat sich in den letzten Jahren von einem Nischenmarkt für Versicherer für den Einkauf von Deckungskapazität nach Katastrophenereignissen zu einem festen Bestandteil des Risikomanagements von Versicherern entwickelt. Durch die Weiterentwicklung der verschiedenen Instrumentarien und die steigende Kapitalkapazität wird ART als Bestandteil von Risikolösungskonzepten immer wichtiger und vielfältiger. Dies betrifft nicht nur den Erst- und Rückversicherungsbereich zur Erschließung neuer Kapazitäten und Diversifizierung, sondern auch immer mehr die Nutzung durch Industrieunternehmen, deren Risiken am traditionellen Markt nicht oder nicht mit der gleichen Effizienz platziert werden können.

Durch die anhaltende Niedrigzinsphase stellt der Insurance-Linked-Securities-Markt für Investoren eine attraktive Anlagemöglichkeit dar. Obwohl das Jahr 2017 durch die beiden Hurrikane „Harvey“ „Irma“, zwei starke Erdbeben in Mexico und die kalifornischen Waldbrände für die Investoren in den ILS-Markt sehr schadenbelastet war, ist der ILS-Markt von 2017 auf 2018 auf 98 Milliarden US-Dollar (ein Wachstum um ca. 10,2 Prozent) gestiegen (vgl. Schultz 2018, S. 5). Der Markt der Insurance-Linked-

Tab. 19.3 Beispiel für die Struktur eines ILW-Vertrages orientiert an (vgl. Soar et al. 2013, S. 5)

Territorium	Risiko	Zeitraum	Limit (USD)	Prämie (USD)	Industrie Trigger (USD)	Individueller Schaden (USD)	Index
USA	Sturm	01.01.– 31.12.2018	10 Mio.	1 Mio.	18 Mrd.	15 Mio.	PCS

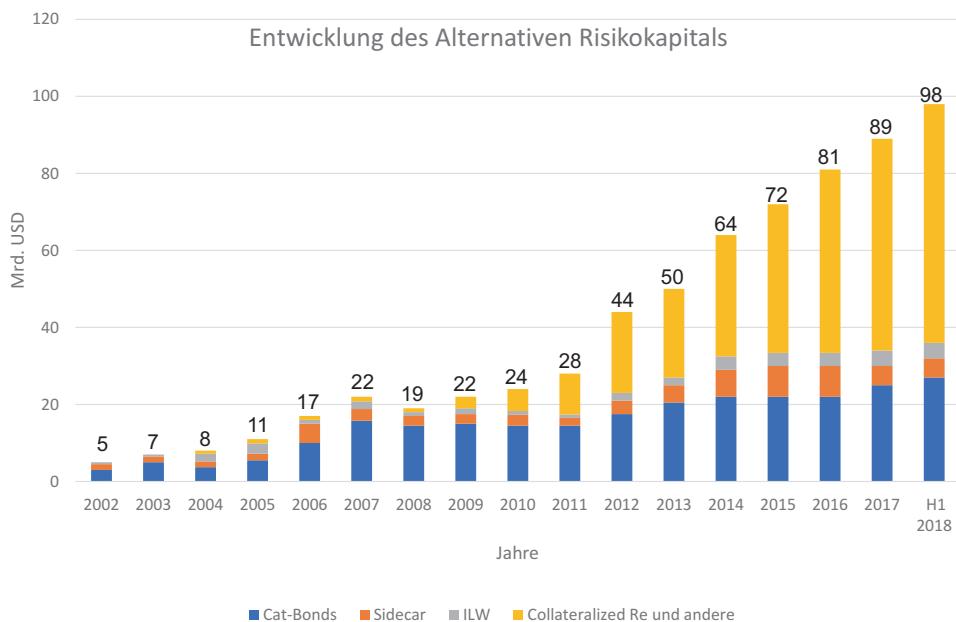


Abb. 19.5 Entwicklung des Alternativen Risikokapitals. (Quelle: eigene Darstellung in Anlehnung an Aon Securities Inc. 2018)

Securities hat somit den ersten Belastungstest bestanden und sich so weiterhin für Investoren als attraktiv erwiesen. Jedoch ist fraglich, ob Ereignisse in dieser Größenordnung einen tatsächlichen Belastungstest für die für die Produkte und die Risikobereitschaft der Investoren darstellen können.

Entscheidend für die weitere Entwicklung des ART (vgl. Abb. 19.5) sind insbesondere zwei Faktoren:

Der erste Faktor ist die Bereitstellung von Kapital durch Investoren. Darauf hat insbesondere die Entwicklung der zu zahlenden Entschädigungsleistungen der Investoren großen Einfluss. Trotz des schadenreichen Jahres 2017 haben sich die Investoren dazu entschieden, weiter in ILS zu investieren, da die bisher erwirtschaftete Rendite diesen Verlust auffängt. Sollten sich aufgrund erhöhter Schadenfrequenz und – Höhe die Investmentmöglichkeiten in den Versicherungsmarkt als unattraktiv herausstellen, werden die Investoren ihr Kapital aus den entsprechenden Bereichen abziehen. Dies würde zu einer erhöhten Nachfrage von traditioneller Rückversicherung führen. Dabei wäre aufgrund mangelnder Alternativen eine Preiserhöhung wahrscheinlich.

Der zweite Faktor stellt das Verhalten der Investoren bei einem möglichen Ende der Niedrigzinsphase dar. Sobald eine attraktivere und risikoärmere Anlagentmöglichkeit vorhanden ist, wird die Motivation der Investoren, in den Versicherungsmarkt zu investieren, vermutlich abnehmen. Dies würde wiederum zu einer erhöhten Rückversicherungsnachfrage und entsprechenden Preissteigerungen führen.

Insgesamt lässt sich sagen, dass Alternativer Risikotransfer in den letzten Jahren deutlich an Wichtigkeit gewonnen hat und (nach derzeitiger Einschätzung) in den nächsten Jahren noch weiter gewinnen wird.

Literatur

- Ali Ishaq. (2005). Reinsuring for catastrophes through industry loss warranties – A practical approach. <https://www.casact.org/pubs/forum/05spforum/05spforum.pdf>.
- Batten, et al. (Hrsg.). (2012). *Derivative securities pricing and modelling* (1. Aufl.). Bingley: Emerald (Emerald books, 94).
- Ben Ammar, et al. (2015). *Alternative risk transfer and insurance-linked securities. Trends, challenges and new market opportunities*. St. Gallen: Institute of Insurance Economics I.VW-HSG University of St. Gallen (I-VW-HSG-Schriftenreihe, Band 56).
- Cummins, et al. (2009). Convergence of insurance and financial markets: Hybrid and securitized risk-transfer solutions. *Journal of Risk and Insurance*, 76(3), 493–545. <https://doi.org/10.1111/j.1539-6975.2009.01311.x>.
- Cummins, et al. (2013). Innovations in insurance markets: Hybrid and securitized risk-transfer solutions. In G. Dionne (Hrsg.), *Handbook of insurance* (S. 547–602). New York: Springer.
- Damjanovic, I., Aslan, Z., & Mander, J. (2010). Market-implied spread for earthquake CAT bonds: Financial implications of engineering decisions. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, 30(12), 1753–1770. <https://doi.org/10.1111/j.1539-6924.2010.01491.x>.
- Eickstädt, J. (2001). *Alternative Risikofinanzierungsinstrumente und ihr Beitrag zur Lösung aktueller Probleme der Industriever sicherung*. München: Gerling-Akad.
- Flämig, M. (2007). *Alternativer Risiko-Transfer – eine volkswirtschaftliche Betrachtung*. @Bamberg, Univ., Diss, 2008. Otto-Friedrich-Universität Bamberg. <http://www.opus-bayern.de/uni-bamberg/volltexte/2009/165/>.
- Gottwald, M. (2015). Lebensrückversicherung im Jahr 2015. https://werde-aktuar.de/Documents/2015_Vortrag_Gottwald.pdf.
- Kailan Shang. (2013). Understanding contingent capital. https://www.casact.org/research/understanding_contingent_capital_complete.pdf. Zugegriffen am 28.07.2018.
- Kuck, A. (2000). *Abgrenzung traditioneller Rückversicherung von Katastrophenrisiken zu ausgewählten Konzepten des alternativen Risikotransfers*. Karlsruhe: VVW. (Veröffentlichungen des Seminars für Versicherungswissenschaft der Universität Hamburg und des Vereins zur Förderung der Versicherungswissenschaft Reihe C, Versicherungs- und Finanzmathematik, 1).
- Laudage, B. (2009). *Aufsicht über strukturierte Rückversicherungskonzepte*. Karlsruhe: VVW. (Versicherungswissenschaft in Berlin : Schriftenreihe des Vereins zur Förderung der Versicherungswissenschaft an der Freien Universität Berlin, der Humboldt-Universität zu Berlin und der Technischen Universität Berlin e. V., Band 33).
- Liebwein, P. (2009). *Klassische und moderne Formen der Rückversicherung* (2. Aufl.). s.l.: Versicherungswirtschaft GmbH. <http://gbv.eblib.com/patron/FullRecord.aspx?p=1204281>.
- Liebwein, P. (2018). *Klassische und moderne Formen der Rückversicherung* (3. Aufl.). Karlsruhe: Versicherungswirtschaft. <https://ebookcentral.proquest.com/lib/gbv/detail.action?docID=5310327>.
- Müller, et al. (2000). Wetterderivate zur Absicherung von Wetterrisiken. Spekulationsinstrument oder Bestandteil des risikopolitischen Instrumentariums in wettersensiblen Branchen? Unter Mitarbeit von Grandi, Marcel. Hg. v. The Geneva Papers on Risk and Insurance. Issues and Practice (No. 2). <https://riva-online.com/wp-content/uploads/2012/11/Grandi-Mueller-Wetterderivate.pdf>. Zugegriffen am 05.08.2019.

- Nguyen, T. (2007). *Grenzen der Versicherbarkeit von Katastrophenrisiken. Erweiterungsmöglichkeiten durch Rückversicherung, Katastrophenanleihen und Versicherungsderivate* (Zugl.: Hagen, FernUniv. Hagen, Habil.-Schr., 2007, 1. Aufl.). Wiesbaden: Deutscher Universitätsverlag (Wirtschaftswissenschaft). <https://doi.org/10.1007/978-3-8350-9612-7>.
- Njegomir, et al. (2009). Risk transfer solutions for the insurance industry. *Ekon. an*, 54(180), 57–90. <https://doi.org/10.2298/EKA0980057N>.
- Polacek, A. (2018). Catastrophe bonds: A primer and retrospective. *CFL*. <https://doi.org/10.21033/cfl-2018-405>.
- Riedler, et al. (2013). *Wetter-und Katastrophenderivate* (Hrsg. v. Zentrum für Europäische Wirtschaftsforschung). https://scholar.google.de/scholar?q=related:JpJkvzncOLEJ:scholar.google.com/&hl=de&as_sdt=0,5. Zugegriffen am 25.07.2018.
- Schultz, P. (2018). *Insurance-linked securities. Alternative capital fortifies its position* (Hrsg. v. Aon Securities). <http://thoughtleadership.aonbenfield.com/Documents/20180905-securities-ils-annual-report.pdf>.
- Schwepcke, A., et al. (2017). *Handbuch der Rückversicherung*. Karlsruhe: Versicherungswirtschaft. <https://ebookcentral.proquest.com/lib/gbv/detail.action?docID=4891989>.
- Schwillig, W. (2018). *Formen und Wirkungen der (obligatorischen) Schaden-/Unfall-Rückversicherung – eine Einführung* (Hrsg. v. Deutsche Rückversicherung AG). https://www.deutscherrueck.de/fileadmin/user_upload/Einfuehrung-RV-Formen_Werner_Schwillig_.pdf. Zugegriffen am 22.06.2019.
- Soar, et al. (2013). *Insurance & reinsurance. A legal guide to industry loss warranty contracts* (Unter Mitarbeit von Kiran Soar, Simon Cooper, Jan Heuvels, Johanna Ewen und Lorraine Fernandes. Hrsg. v. Ince&Co). <https://www.incegd.com/file.axd?pointerid=59144cd603996f0de4f0357b>. Zugegriffen am 06.08.2019.
- Wagner, F. (2008). *Gabler Lexikon Versicherung* (1. Aufl.). Wiesbaden: Betriebswirtschaftlicher Verlag Gabler.
- Young, J. B. (1991). Risk financing alternatives – Size and impact on the commercial insurance market. *RMR*, 5(18), 15–24.
- Zeller, W. (2008). Securitization and insurance – characteristics of Hannover Re's approach. *Geneva Papers on Risk and Insurance – Issues and Practice*, 33(1), 7–11. <https://doi.org/10.1057/palgrave.gpp.2510166>.

Ralf Weyand (geb. 1973 in Köln) absolvierte zunächst eine Ausbildung zum Versicherungskaufmann bei der Allianz in Köln, bevor er an der Universität zu Köln Betriebswirtschaftslehre mit Schwerpunkten in Statistik und Versicherung studierte. Seit 2001 ist Herr Weyand bei der Hannover Rück beschäftigt, wo er sich seit 2002 der strukturierten Rückversicherung widmet. Seit April 2019 leitet Herr Weyand den Zentralbereich Advanced Solutions, der mit einem Volumen von ca drei Milliarden Euro und zwei Teams in Hannover und Dublin weltweit zu den führenden Anbietern von strukturierten und maßgeschneiderten Rückversicherungslösungen zählt.

Mathis Herzke studierte den Bachelor Versicherungswesen mit den Schwerpunkten Sach- und Betriebsunterbrechungsversicherung, Betriebliches Risiko- und Schadenmanagement sowie Organisation und Informationsverarbeitung des Versicherungsbetriebsam Institut für Versicherungswesen(ivwKöln). Während des Bachelorstudiums verbrachte er ein Auslandsjahr an der University of Limerick mit dem Fokus auf Business Consulting, Underwriting und International Insurance. Im Anschluss absolvierte er am ivwKöln den Master Risk & Insurance. Während des Studiums war er für die Ecclesia Gruppe, die Scor und Victor Insurance tätig. Seit Oktober 2020 ist Herr Herzke bei der Deutschen Familienversicherung als Referent für Produktentwicklung tätig.

Teil V

Risiken, Risikomanagement und Versicherungsaspekte



Internationale Versicherungsprogramme

20

Oder: Wie international tätige Unternehmen ihre Risiken in den Griff bekommen

Rüdiger Auras und Michael Dehm

Zusammenfassung

Internationale Versicherungsprogramme sind in unserer globalisierten Welt nicht mehr wegzudenken und ein fester Bestandteil in der Industriever sicherung. Sie gibt es in den verschiedenen Sparten in unterschiedlichen Ausprägungen. Die Gestaltung folgt nicht nur den Anforderungen der Versicherungsnehmer, sondern unterliegt auch den von Land zu Land unterschiedlichen aufsichts- und steuerrechtlichen Regelungen. Für die Herausforderungen, die bei der Gestaltung eines Internationalen Versicherungsprogrammes auf Versicherungsnehmer, Makler und Versicherer zukommen, gibt es verschiedene Lösungsansätze, die ihre Vor- und Nachteile haben.

20.1 Einleitung

Auslöser für die Nachfrage nach Internationalen Versicherungsprogrammen ist die zunehmende Globalisierung, der damit verbundene weltweite Handel und die zunehmende Verlagerung von Produktionsprozessen aus dem Mutterland eines Unternehmens hinaus in andere Länder. So stieg das Welthandelsvolumen im Zeitraum von 1970 bis 2014 von 0,3 auf 18,9 Billionen US-Dollar (Handel und Investitionen, aus: Zahlen und Fakten: Globalisierung, Bundeszentrale für politische Bildung/bpb), die Zahl der direkten Auslandsinvestitionen im gleichen Zeitraum von 13 auf rund 1400 Milliarden US-Dollar (vgl. Ausländische Direktinvestitionen (ADI) pro Jahr, aus: Zahlen und Fakten: Globalisierung, Bundeszentrale für politische Bildung/bpb).

R. Auras (✉) · M. Dehm
Aon, Mülheim an der Ruhr, Deutschland
E-Mail: ruediger.auras@aon.de; michael.dehm@aon.de

Die heutige Industrie, und insbesondere die der exportstarken Länder wie Deutschland, benötigt für ihre spezialisierten und qualitativ hochwertigen Waren Märkte, die die Nachfrage ihrer heimischen Volkswirtschaft übertreffen. Diese Märkte befinden sich sowohl in anderen Industrieländern, als auch in Entwicklungs- und Schwellenländern. Industriestaaten sind deshalb in der Regel für die Öffnung von Märkten. Dem gegenüber stehen staatliche Interessen. Staaten sind auf Steuereinnahmen angewiesen, die von im Land angesiedelten Unternehmen und den Beschäftigten in Form direkter und indirekter Steuern gezahlt werden. Verlagerungen von Unternehmenstätigkeiten sind von daher nicht immer erwünscht, können sie doch zu unliebsamen Veränderungen führen. Unternehmen dagegen wählen Standorte häufig abhängig von der Nachfrage, von der Höhe der Lohnkosten (zum Beispiel in Entwicklungs- und Schwellenländern), aber auch nach der Steuer- und Abgabenbelastung aus.

Heute produzieren viele Unternehmen weltweit (Global Players) und haben so die Möglichkeit, die unterschiedlichen Arbeitskosten, Investitions-, Steuer- und sonstige Bedingungen in den unterschiedlichen Ländern zu ihren Gunsten zu nutzen. National operierende kleinere Unternehmen, die diese Möglichkeiten zunächst nicht haben, sind durch die Konkurrenz international operierender Unternehmen vielfach in ihrer Existenz bedroht. Viele sehen sich gezwungen, ihrerseits Arbeitsplätze in Niedriglohnländer zu verlegen, was wiederum negative Rückwirkungen auf Arbeitsmärkte und heimische Nachfrage in Hochlohnländern haben kann und die Globalisierung weiter vorantreibt. Nach Schätzungen sind multinationale Unternehmen an ca. zwei Dritteln des Welthandels beteiligt und ca. ein Drittel des Welthandels findet direkt zwischen Mutter- und Tochterunternehmen von Konzernen, also „intra-firm“ statt (vgl. UNCTAD 2002, S. 153).

Ob dieser Trend anhält, ist zumindest fraglich. Eine Studie des HWWI und der Beerenberg Bank aus dem Jahr 2018 rechnet in der näheren Zukunft (bis ca. 2030) mit einem Rückgang globaler Wertschöpfungsketten und weltweiter Transporte von Fertigprodukten (vgl. Quitzau et al. 2018). Auch die durch den Corona-Virus SARS-CoV 2 Anfang 2020 ausgelöste Pandemie wird sicherlich bei vielen zu Überlegungen führen, ob und in welchem Umfang eine weitere Ausbreitung globaler Wertschöpfungsketten Sinn macht.

20.2 Auswirkungen der Globalisierung auf die Industriever sicherung

Global tätige Industrieunternehmen haben von Beginn der Globalisierung an versucht, möglichst einheitlichen und umfassenden Versicherungsschutz für ihre weltweiten Risiken, üblicherweise basierend auf dem ihnen bekannten Versicherungsschutz ihres Heimatmarktes, zu erlangen. Dabei sollte der Einkauf dieses Versicherungsschutzes schlank, das heißt mit wenig administrativem Aufwand, verbunden sein. Er sollte eine möglichst einheitliche Schadenregulierung weltweit bieten und lokalen Service im gewünschten Umfang gewähren. Dies alles unter Einhaltung aufsichts- und steuerlicher Regelungen, auch wenn diese Frage zu Beginn zunächst noch keine bedeutende Rolle einnahm.

Bereits Ende der Fünfzigerjahre des vorigen Jahrhunderts haben deshalb große Industriever sicherer in den USA und Europa, hier vor allem in Großbritannien, sogenannte

„Internationale Versicherungsprogramme“ (IVP) entwickelt. In Deutschland wurden die ersten IVP allerdings erst in den Siebzigerjahren des vorigen Jahrhunderts angeboten (vgl. Farny 1984, S. 31). Die seither stark zunehmende Globalisierung hat dann vor allem in den Achtzigerjahren zu einer erheblichen Internationalisierung des Versicherungsgeschäfts im Industriesektor geführt (vgl. Woltereck 1988, S. 13 und 15).

Heute müssen international tätige Unternehmen eine Vielzahl von Herausforderungen bewältigen. Eine dieser Herausforderungen ist es, alle Standorte und Tätigkeiten des Unternehmens mit länderübergreifenden Versicherungslösungen abzusichern. Es gilt, an jedem Standort im Ausland die Bereitstellung von Produkten und Dienstleistungen in ein Versicherungsmanagement einzubinden, das mit dem Risikomanagement und der Risikophilosophie des gesamten Konzerns verzahnt ist: eine Mammutaufgabe für die Unternehmen.

Gleichzeitig haben sich die Risiken für Unternehmen durch die fortschreitende Internationalisierung kontinuierlich erhöht. Damit hat auch die Bedeutung korrespondierender Versicherungslösungen stetig zugenommen.

Auch die Arbeitsweise der Unternehmen hat sich verändert, was die Absicherung von Risiken schwieriger gemacht hat. Veränderungen in der Produktionsweise, zunehmende Modularisierungen bei der Herstellung des Endprodukts mit internationalen Zuständigkeiten im eigenen Konzern und eine große Zahl an Zulieferern aus verschiedenen Ländern: All das hat dazu geführt, dass sich in vielen Unternehmen die Wertschöpfungskette über Kontinente hinweg erstreckt und die individuelle Risikosituation aller am Prozess Beteiligten kaum noch vollständig erfasst geschweige denn kontrolliert oder beherrscht werden kann. Auch kleinere mittelständische Unternehmen müssen daher heute anspruchsvollen Versicherungsherausforderungen gerecht werden, die früher nur von multinationalen Großkonzernen bewältigt werden mussten.

Damit sind die Anforderungen an IVP risikoseitig und versicherungstechnisch so individuell, wie es die weltweite Aufstellung und Produktion des jeweiligen Unternehmens notwendig macht.

20.3 Regulierung

In dieser ohnehin schon anspruchsvollen Situation tragen zunehmend die konsequenter formulierten Compliance-Anforderungen an internationale Versicherungslösungen zu einer Verschärfung der Situation bei: Viele der ehemals praktizierten Absicherungskonzepte weisen heute regulatorische Lücken auf oder bergen zumindest gewisse Unsicherheiten.

Nicht erst seit Einführung entsprechender versicherungstechnischer Lösungen durch international tätige Versicherungsunternehmen ist die Regulierung und das Einhalten aufsichts- und steuerrechtlicher Vorgaben (Stichwort: „Compliance“) bei der Gestaltung internationaler Versicherungsprogramme ein bedeutsames Thema für Versicherer, Makler und vor allem auch die Versicherungsnehmer. Die zunehmende Sensibilität der Aufsichts- und Steuerbehörden, dazu einige praktische Fälle, in denen vor allem im Rahmen der Schadenabwicklung Vorwürfe über Verstöße gegen Aufsichts- und/oder Steuerrecht aufkamen, haben zu einer weitreichenden Verunsicherung in der (Versicherungs-)Industrie geführt.

Grund hierfür ist eine mehr oder weniger protektionistische Realität. Dies ist mehreren Faktoren geschuldet: Zum einen haben in der Regel, und dies weltweit, die lokalen Aufsichts- und Steuergesetzgebungen IVP und die daraus folgenden Herausforderungen nicht im Fokus. Die lokalen Regelungen tragen üblicherweise Besonderheiten des lokalen Versicherungsmarktes Rechnung und das Aufsichtsrecht dient zumeist dem Schutz der privaten Verbraucher im Land. Darüber hinaus spielt aber auch der Schutz der eigenen Versicherungsindustrie eine Rolle und letztendlich fürchten gerade Schwellenländer durch im Ausland eingekaufte Versicherung im Rahmen von IVP einen Kapitalabfluss. Aber selbst, wenn grenzüberschreitende Versicherung zugelassen ist, gibt es Hemmnisse. So bezieht sich die Zulassung in manchen Fällen nicht auf mit der Versicherung verbundene Dienstleistungen wie zum Beispiel Risikobesichtigungen oder Schadenbearbeitung durch im Ausland sitzende Versicherer. Ein Beispiel hierfür waren die Flutschäden in Thailand im Jahr 2011. Hier führten Restriktionen in Bezug auf Schadenbearbeitung und Schadenzahlungen zu Verzögerungen bei der Schadenregulierung von bis zu 18 Monaten.

Erschwerend kommt hinzu, dass die Zuständigkeiten der Aufsichtsbehörden von Land zu Land unterschiedlich geregelt sind und sich teilweise erheblich voneinander unterscheiden. Ist in einem Land die Belegenheit des Risikos für die aufsichtsrechtliche Zuständigkeit verantwortlich, so richtet sich dies im nächsten Land danach, wo der Vertrag abgeschlossen wurde.

Gleichzeitig muss das IVP, wie zuvor erläutert, allen gesetzlichen, also auch aufsichts- und steuerrechtlichen Regularien der jeweils einbezogenen Länder entsprechen. Denn nur dann kann die Versicherungslösung auch im fernen Ausland leisten, wofür sie als bedeutender Bestandteil der Risikovorsorge eines Unternehmens vorgesehen ist; nämlich substantiellen Bilanzschutz durch den Transfer versicherbarer Risiken zu gewähren. Zudem werden damit nicht nur Unternehmensinteressen gewahrt, sondern auch strenge gesetzliche Anforderungen bedient, wie sie in Deutschland beispielsweise im Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) begründet sind.

20.4 IVP als wichtiges Instrument – Erscheinungsformen und Herausforderungen

Aus deutschem Blickwinkel handelt es sich bei einem IVP um eine von der deutschen Muttergesellschaft abgeschlossene länderübergreifende Versicherungslösung, mit der versicherbare und als versicherungswürdig identifizierte Interessen der Muttergesellschaft und der ausländischen Tochtergesellschaften gedeckt werden. Somit steht das IVP im Gegensatz zu eigenständigen und nicht miteinander koordinierten Versicherungslösungen der jeweiligen Tochtergesellschaften im Ausland. Diese sogenannten „Stand-alone-Deckungen“ sind zwar unter Compliance-Gesichtspunkten als weitestgehend unproblematisch zu bewerten. Jedoch bergen sie erhebliche Nachteile aus Sicht des Gesamtunternehmens und vor allem auch der Unternehmenszentrale. Sie sind weitgehend intransparent, Deckungslücken sind praktisch unvermeidbar, grenzüberschreitende Risiken können nicht oder nur bedingt abgesichert werden. Dazu kommt ein sehr hoher Koordinationsbedarf und administrativer Aufwand, letztendlich muss die Deckung in jedem

Land individuell ausgeschrieben und verhandelt werden. Aufgrund geringer Transparenz, hohen Kosten und weltweit nicht konsistentem Versicherungsschutz spielen „Stand-alone-Deckungen“ in der Praxis daher nur noch eine untergeordnete Rolle.

Unter dem Sammelbegriff IVP hat sich eine Reihe von Varianten herausgebildet und etabliert. Sie beschreiben unterschiedliche Deckungskonzepte und ein jeweils unterschiedliches Zusammenspiel zwischen dem Hauptvertrag in Deutschland (dem Mastervertrag) und den Lokalpolicen im Ausland.

Unabhängig von der endgültigen Ausgestaltung stellt sich bei der rechtlichen Betrachtung dieser versicherungstechnischen Konstrukte immer die Frage nach der rechtlichen Zuständigkeit. Es gibt Berührungspunkte zu einer Vielzahl von Rechtsordnungen. Insbesondere die Frage, welchem materiellen Recht der Mastervertrag unterliegt und vor welchem Gericht dieses Recht von den Parteien geltend gemacht werden kann, ist dabei von Interesse. Für die lokalen Polices ergeben sich derartige Fragestellungen eher nicht, da diese vor Ort zwischen einem lokalen Versicherungsunternehmen und dem Tochterunternehmen des Versicherungsnehmers des Mastervertrages geschlossen werden. Sie unterliegen damit dem dortigen Versicherungsvertragsrecht (vgl. hierzu Mächler-Erne 2000, S. 153 und 163; vgl. Basedow und Scherpe 2005, S. 511 und 518).

Interessanter stellt sich jedoch, wie bereits angedeutet, die Situation im Hinblick auf den Mastervertrag dar, der Risiken in einer Vielzahl von Ländern abdeckt und somit auch Berührungspunkte zu einer großen Anzahl von Rechtsordnungen aufweist. Die sich daraus ergebenden Fragestellungen sind vielfältig und komplex und auch nach Sparten gegebenenfalls unterschiedlich.

20.4.1 Lösungen ohne Lokalpolicen: „Freedom of Services“, „non admitted“-Deckungen und Absicherung des eigenen finanziellen Interesses über Wertverlustklauseln

Im Rahmen der Dienstleistungsfreiheit zwischen Ländern (Freedom of Services oder auch FoS) kann Versicherungsschutz, wie zum Beispiel in der Europäischen Union, ohne Beschränkungen grenzüberschreitend zur Verfügung gestellt werden, auch wenn die nationalenaufsichtsrechtlichen Bestimmungen eigentlich etwas anderes vorsehen. Solche Lösungen sind jedoch die Ausnahme.

Länder, die für die klassische Struktur eines IVP kritisch sind, weil sie grenzüberschreitende Versicherung und damit zusammenhängende Dienstleistungen nicht zulassen, werden als Verbotsstaaten (oder auch sogenannte „Non admitted Countries“) bezeichnet. Allerdings ist dieser Begriff missverständlich. Es geht nicht nur um die Frage, ob ein Land den Betrieb von Versicherungsgeschäft durch einen nicht zugelassenen Versicherer untersagt, denn dies trifft auf die meisten Länder, die über ein Versicherungsaufsichtsrecht verfügen, zu (vgl. Strnad 2007, S. 345 und 346; vgl. Mazenauer 2008, S. 19 und 20; vgl. Armbrüster 2008, S. 853; vgl. Kasper 2008, S. 2). Vielmehr ist danach zu differenzieren, an welche Tatbestände Länder ihre Aufsichtspflicht knüpfen. Verbotsländer sind demnach diejenigen Staaten, die eine Unterwerfung unter ihr eigenes Aufsichtsrecht bereits dann

fordern, wenn ausländische Versicherer und Versicherungsnehmer im Ausland über ein im Inland belegenes Risiko einen Versicherungsvertrag abschließen (richtig und mit vergleichbarem Ansatz Langheid und Grote 2008, S. 630 und 632; vgl. Laupichler und Post 2008, S. 914; vgl. Bähr und Püttgen 2008, S. 1078; vgl. Mahnke 2008, S. 8 und 9; vgl. Koch 2009, S. 141; vgl. Bialowons und Kerst 2011, S. 317; vgl. jetzt auch Strnad 2009, S. 1263 und 1266). Ebenso sind diejenigen Länder zu qualifizieren, deren Aufsichtspflicht zwar nicht direkt an die Risikobelegenheit anknüpft, im Ergebnis jedoch zu einer ähnlichen Beschränkung des grenzüberschreitenden Versicherungsverkehrs führt.

Ein reines „non admitted“-Konzept sieht nur einen Vertrag vor, in der Regel im Mutterland des Unternehmens, in unserem Beispiel in Deutschland. Es umfasst keine Lokalpolicien und exportiert sozusagen den nach deutschem Recht formulierten Versicherungsschutz aus diesem Vertrag, auch Mastervertrag genannt, in die mitversicherten Länder. Damit erfolgen die komplette Administration sowie eine eventuelle Schadenabwicklung grundsätzlich aus Deutschland heraus. Zwar besteht weltweit Versicherungsschutz auf Basis einheitlicher Bedingungen, Besonderheiten anderer Märkte finden hierbei jedoch keine Berücksichtigung. Auch basiert dieser Versicherungsschutz auf Bedingungen nach deutschem Recht, andere gesetzliche Vorschriften und Regeln können nicht oder nur bedingt abgebildet werden.

Dieses Deckungskonzept findet spätestens dort seine Grenzen, wo „non admitted“-Deckungen nicht zulässig sind – wie zum Beispiel in der Schweiz oder in China. Entsprechend kann die Schadenbearbeitung und -regulierung von Schäden im Ausland, sei es durch einen involvierten Makler oder Sachverständigen oder den Versicherer selbst, rechtlich problematisch sein. Neben einem Verstoß gegen das lokale Aufsichtsrecht liegt dann möglicherweise auch ein Verstoß gegen die Rechtsdienstleistungsgesetzgebung vor. Denn der den Schaden regulierenden Makler, Sachverständige oder sonstige Beauftragte kann sich in diesen Fällen unter Umständen nicht wie üblich auf seine Annexkompetenz berufen, da er die Hauptleistung (Vermittlung des Versicherungsvertrages) im Ausland, wo der Schaden belegen ist, nicht erbracht hat. Weiterhin werden in solchen Fällen, wenn Schadenzahlungen ins Ausland transferiert werden, auch die Steuerbehörden aufmerksam und prüfen, ob hier ein Steuerumgehungstatbestand erfüllt ist.

Dies trifft im Übrigen auch für die Fälle zu, in denen FoS oder „non admitted“-Deckungen erlaubt sind, da sich dies in der Regel nur auf das Aufsichtsrecht bezieht, die steuerlichen Regelungen davon aber ausgenommen sind. So sind selbst innerhalb der Europäischen Union, in der FOS-Programme erlaubt sind, die lokal gültigen Steuern in den Ländern, in denen die betroffenen Risiken belegen sind, abzuführen.

Im Zusammenhang mit der Diskussion über die länderübergreifende Anwendbarkeit von DIC-/DIL-Deckungen hat sich mit der sogenannten „Financial Interest Coverage“ (FInC), auch Versicherung des Finanzinteresses genannt, ein weiterer Ansatz zum Umgang mit der Verbotsstaatenproblematik entwickelt (vgl. hierzu Strnad 2007, S. 345 und 350; vgl. Strnad 2008, S. 15 und 18; vgl. Mazenauer 2008, S. 19 und 21; vgl. Laupichler und Post 2008, S. 914; vgl. Bähr und Püttgen 2008, S. 1078). Grundsätzlich ändert sich durch die Vereinbarung einer FInC-Klausel nichts an der Programmgestaltung eines IVP. Es wird lediglich zusätzlich zu der klassischen DIC-/DIL-Deckung eine Vereinbarung für den Fall aufgenommen, dass diese rechtlich nicht zulässig sind. In diesem Fall wird der angenom-

mene, finanzielle Schaden der Muttergesellschaft (Wertverlust) durch ein im Ausland eingetretenes Schadenereignis bei einem Tochterunternehmen oder einer Niederlassung versichert. Soweit möglich folgt die Schadenregulierung der klassischen DIC-/DIL-Deckung. Auch hier achten die Versicherungsunternehmen darauf, dieses Konzept möglichst sparsam einzusetzen und zunächst die Möglichkeiten der herkömmlichen Versicherungsdeckung maximal auszuschöpfen (vgl. Strnad 2007, S. 345 und 348 f.; vgl. Strnad 2008, S. 15 und 17 f.; vgl. Strnad 2009, S. 1263, 1270; vgl. Bähr und Püttgen 2008, S. 1078 f.; vgl. Langheid und Grote 2008, S. 1510). Dabei ist zu berücksichtigen, dass im Rahmen einer FInC-Deckung eine Schadenregulierung vor Ort üblicherweise nicht oder nur unter erschwerten Umständen möglich ist, da lokal ja kein versicherter Schaden eingetreten ist.

Ansonsten bleibt aber das Zusammenspiel aus lokalen Polices und Mastervertrag erhalten (vgl. Strnad 2007, S. 345 und 350; vgl. Strnad 2008, S. 15 und 18; vgl. Strnad 2009, S. 1263 und 1274 f.; vgl. Mazenauer 2008, S. 19 und 21; vgl. Kasper 2008, S. 2; vgl. Laupichler und Post 2008, S. 914; vgl. Bähr und Püttgen 2008, S. 1078 f.).

20.4.2 IVP als koordiniertes Programm

Ein koordiniertes Programm verfügt über lokal abgestimmten und platzierten Versicherungsschutz, der nicht integrierter Teil des internationalen Programms ist. Das heißt, die lokale Deckung steht separat und mit eigenständiger Kapazität zur Verfügung. Der Mutterkonzern gibt einen Mindeststandard an Versicherungsschutz vor, der lokal einzukaufen ist. Auf dieser Basis wird lokal der Versicherungsschutz vereinbart, der lokale Versicherer wird vom Mutterkonzern nicht vorgegeben und muss nicht der Versicherer des Mastervertrages sein. Der Mastervertrag des Konzerns knüpft jedoch an die Lokalpolice an und bezieht diese in das Programm mit ein. Die Auslandsgesellschaften haben die Möglichkeit, ihnen nahestehende lokale Versicherungsmärkte zu nutzen.

Die Kosten sind aufgrund der zusätzlichen, mehrfach einzukaufenden Kapazitäten üblicherweise höher. Und die Schadenregulierung kann sich bei lokal nicht oder nur unzureichend gedeckten Sachverhalten, die jedoch über den Mastervertrag abgesichert sind, als kompliziert erweisen, wenn mehrere Versicherungsgesellschaften involviert sind.

Entscheidend für den Programmversicherer ist, dass überhaupt eine angemessene Grundversicherung existiert. Daher enthält der Mastervertrag üblicherweise eine Klausel, die einen entsprechend höheren Selbstbehalt einfordert, falls keine lokale Police vorhanden ist oder im Schadenfall der vereinbarte Mindeststandard an Deckung nicht zur Verfügung steht.

20.4.3 IVP als integriertes Programm

Sogenannte „Integrierte IVP“ können in verschiedenen Ausgestaltungen konzipiert werden.

20.4.3.1 Allgemein

Auch bei einem integrierten Programm werden die lokalen Grunddeckungen nach dem Prinzip des „Good Local Standard“ eingerichtet und mit dem Programmversicherer abgestimmt. Die-

ser gibt die Versicherungspartner im Ausland vor – soweit wie möglich eigene Gesellschaften oder etablierte Partnergesellschaften. Die Lokalpolices, die in der Regel zu 100 Prozent durch den Programmversicherer bzw. dessen lokale Tochterunternehmen bzw. durch lokale Fronting Partner ausgestellt werden sind anders als beim koordinierten IVP ein „integrierter“ Bestandteil des Programms und knüpfen direkt an den Mastervertrag an. Sie werden in der Regel über Rückversicherungsverträge im Land des Mutterkonzerns zusammengeführt.

Insbesondere bei der Versicherung internationaler Haftpflichtrisiken werden insoweit keine zusätzlichen bzw. eigenständigen Deckungssummen im Ausland aufgebaut, was ein wesentliches Element der Kosteneffizienz des integrierten IVPs ausmacht (vgl. Abb. 20.1). Die lokal zugeordneten Deckungssummen sind verhältnismäßig niedrig und korrespondieren mit der üblichen Schadenfrequenz in den jeweiligen Ländern.

20.4.3.2 Integriertes Haftpflicht-IVP als „Twin Tower“-Programm

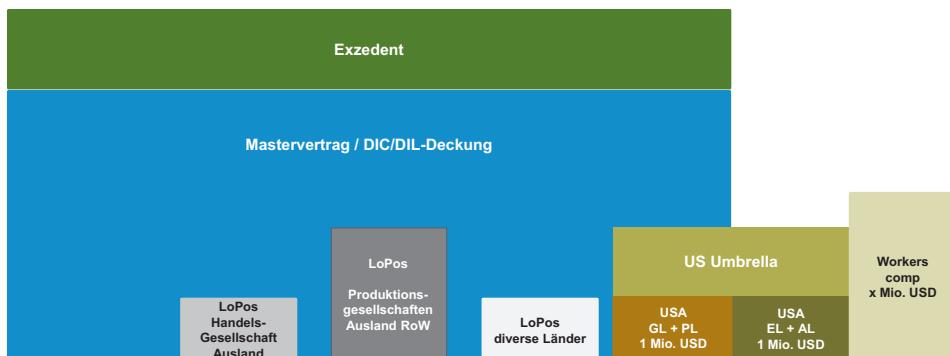
Bei einem sogenannten „Twin Tower“-Programm (vgl. Abb. 20.2) handelt es sich in der Regel um eine Erweiterung eines integrierten IVP. Diese Erweiterung erfolgt, um wichtigen und im Ausland notwendigen Sonderdeckungen Rechnung zu tragen und sie mit höheren eigenständigen Kapazitäten zu versehen, als dies über die normale und integrierte Lokalpolice üblich wäre.

Meistens wird dieses Modell durch lokale regulatorische Bestimmungen erforderlich. Häufig findet man dieses Modell für Haftpflichtrisiken in den USA, wo insbesondere „Auto Liability“, „Employers Liability“ und die „Workers Compensation“ auf diese Weise mit substanziellem eigenen Kapazitäten versehen werden können. Teile davon können über einen zusätzlichen gemeinsamen lokalen „Umbrella“ in der Deckungssumme nochmals erweitert werden. Hieran kann neben einem sogenannten „Following Form Excedenten“ zwecks weiterer Preisoptimierung alternativ auch der deutsche Mastervertrag anknüpfen.

20.4.3.3 Integriertes IVP Sach

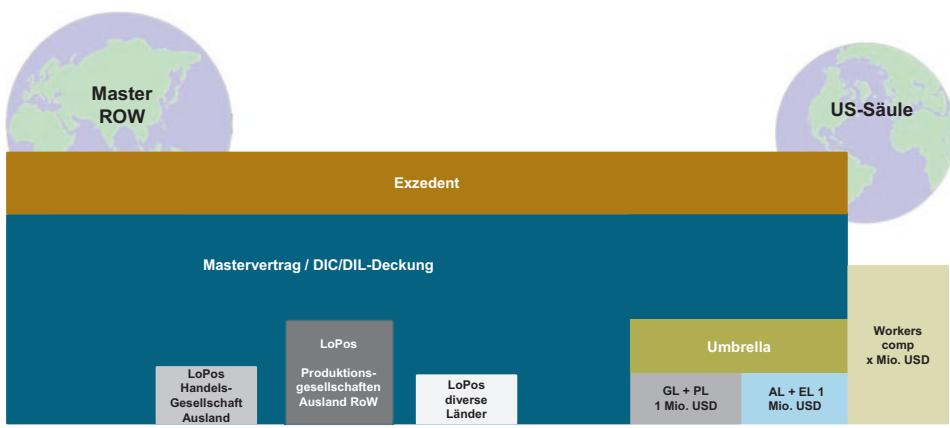
Anders als bei einem Haftpflichtversicherungsprogramm, steht bei einem Sachversicherungsprogramm nicht die Einsparung von Kapazitäten im Vordergrund (vgl. Abb. 20.3). Aber auch hier kann dies eine Rolle spielen, insbesondere der Einkauf von Kapazitäten für die Versicherung von Naturgefahren ist auf diese Weise deutlich effektiver möglich, als im Rahmen von „Stand-alone“-Policen.

Der hauptsächliche Vorteil eines integrierten Sach-IVP ergibt sich aber aus der Mitversicherung von länderübergreifenden Wechselwirkungen zwischen Unternehmensbereichen, dem einheitlichen Versicherungsschutz weltweit, bei dennoch lokaler Deckung, die auch in einzelnen Ländern vorkommenden Besonderheiten Rechnung tragen. Einher geht dies meistens mit einem koordinierten Risk-Engineering-Konzept, entweder durch den führenden Programmversicherer, den Makler oder durch ein drittes, hierauf spezialisiertes Unternehmen. Hier werden neben dem klassischen Brandschutz zunehmend auch Risiken aus dem Betriebsablauf und durch Naturgefahren oder Nebengefahren erfasst. Die Ergebnisse haben häufig einen direkten Einfluss auf die erforderlichen Kapazitäten und die Selbstbehaltssstruktur.



- LoPo – Lokale Police(n)
- GL – General Liability / Allgemeine Haftpflicht
- PL – Products Liability / Produkt Haftpflicht
- EL – Employers Liability (Arbeitgeberhaftpflicht)
- WC – Workers' Compensation / Gesetzliche Unfallversicherung
- AL – Automobile Liability (Kfz-Haftpflicht)
- DIC – Difference in Conditions / Bedingungsdifferenz
- DIL – Difference in Limits / Summandendifferenz

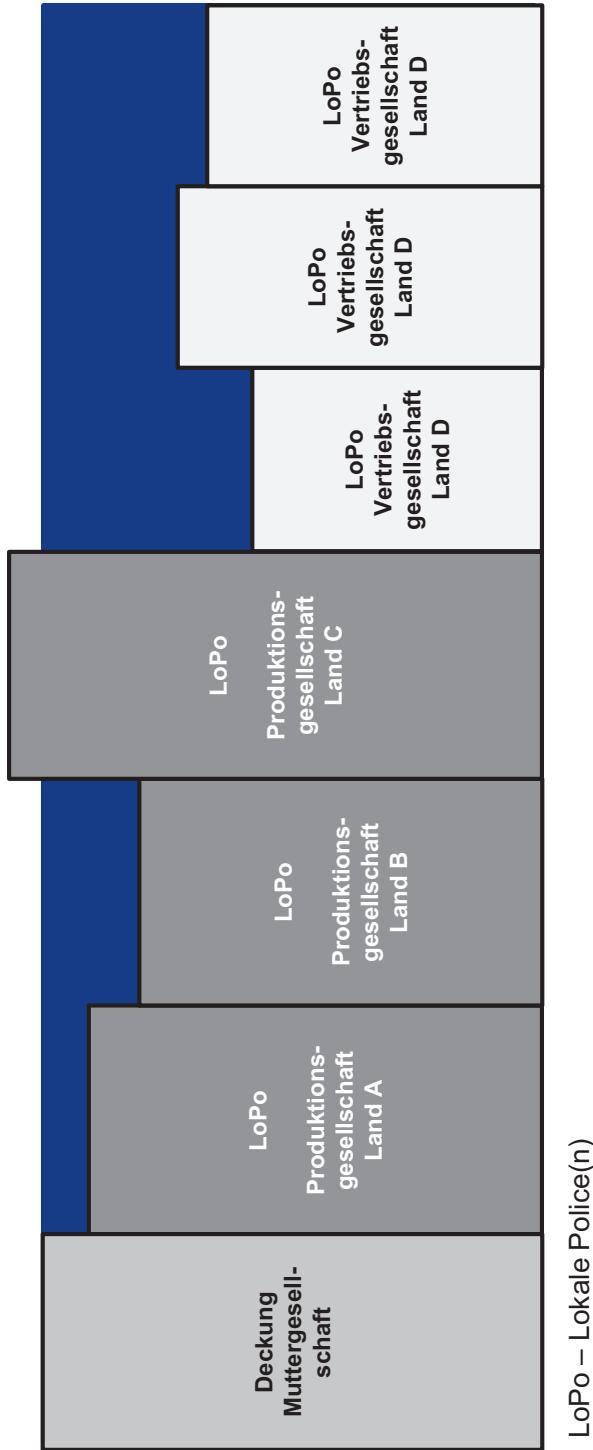
Abb. 20.1 Integriertes IVP Haftpflicht. (Quelle: eigene Darstellung)



- LoPo – Lokale Police(n)
- GL – General Liability / Allgemeine Haftpflicht
- PL – Products Liability / Produkt Haftpflicht
- EL – Employers Liability / Arbeitgeberhaftpflicht
- WC – Workers' Compensation / Gesetzliche Unfallversicherung
- AL – Automobile Liability / Kfz-Haftpflicht
- DIC – Difference in Conditions / Bedingungsdifferenz
- DIL – Difference in Limits / Summandendifferenz

Abb. 20.2 Modified Twin Tower. (Quelle: eigene Darstellung)

Mastervertrag / DIC-/ DIL- oder FInC-Deckung



- **DIC – Difference in Condition / Konditionsdifferenzdeckung**
- **DIL – Difference in Limits / Summandendifferenzdeckung**
- **FInC – Financial Interest Cover / Versicherung des finanziellen Interesses**

Abb. 20.3 Integriertes IVP Sach. (Quelle: eigene Darstellung)

Da es sich im Sachversicherungsbereich um die Versicherung stationärer Risiken handelt, die, sofern FOS- oder „non admitted“-Deckungen nicht zugelassen sind, lokal versichert werden, müssen die Kapazitäten auch lokal eingekauft werden. Ausnahmen gibt es, wie oben genannt, im Naturgefahrenbereich, aber auch im Betriebsunterbrechungsbereich kann der Kapazitätseinkauf im Rahmen eines IVP effizienter gestaltet werden. Weiterhin können im Rahmen eines Sach-IVP lokale Besonderheiten berücksichtigt werden. So ist es beispielsweise möglich, für einzelne Länder Deckungsbausteine aus technischen Versicherungen (zum Beispiel Montage, Bauleistung) im Rahmen der lokalen Deckung einzuschließen, wenn dies gewünscht wird, auch wenn der Mastervertrag diese Deckung eigentlich nicht vorsieht.

Ein weiteres Unterscheidungsmerkmal ist, dass bedingt durch den erforderlichen Einkauf der Kapazitäten im jeweiligen Land der Großteil der Prämie eines Sach-IVP dezentral erhoben wird. Umso wichtiger ist hier die Rückversicherung der Risiken in das Land des Mutterkonzerns, da auf diesem Weg die beteiligten Versicherer bedient werden können.

20.4.3.4 Bewertung

Integrierte Programme sind inzwischen in allen Sparten Standard, allerdings gibt es Mischformen. Vor allem, wenn der Kunde in Regionen und Ländern vertreten ist, in denen der führende Programmversicherer nicht vertreten ist und auch keine Kooperationspartner hat, wird auf lokale Versicherer zurückgegriffen, analog dem Vorgehen bei einem koordinierten Programm.

Grundsätzlich spielt der lokale Versicherer bei einem integrierten IVP weniger die Rolle eines klassischen Versicherers, sondern gleicht eher einem Dienstleister. Der Vertrieb, die Risikobewertung und Preisfindung erfolgen durch den Versicherer des Mastervertrages. Die Hauptaufgabe des lokalen Versicherers besteht darin, Dienstleistungen vor Ort, zum Beispiel im Rahmen der Schadensabwicklung oder bei der Abführung der Versicherungssteuer, zu übernehmen (vgl. Mächler-Erne, S. 153 und 164). Er wird hierfür mit einer entsprechenden Bezahlung, der Fronting Fee oder auch Overrider genannten Gebühr, entlohnt, die Gegenstand der Vereinbarungen zwischen den Versicherern einer Gruppe oder auch zwischen Versicherer und Kooperationspartner ist.

Die lokalen Versicherungsprämien werden soweit zulässig weitestgehend an den Versicherer des Mastervertrages im Rahmen einer fakultativen Rückversicherung zediert. Dieser verteilt diese, sofern das IVP durch mehrere am Mastervertrag in der Regel offen beteiligte Versicherer konzipiert wurde, auf dem Wege einer Retrozession, abzüglich der Gebühren für die administrative Verwaltung, an die Konsorten.

20.4.4 Programmoptimierung im IVP durch Verknüpfungsklauseln

Neben der DIC (Difference in conditions) oder Konditionsdifferenzdeckung, die inhaltliche Deckungslücken zwischen Mastervertrag und Lokalpolicien ausgleicht, und der DIL (Difference in limits) oder Summendifferenzdeckung, die Kapazitätsslücken der Lokalpolicien, die in der Regel niedrigere Deckungssummen haben, ausgleicht, gibt es noch weitere Verknüpfungsklauseln. Sie dienen dazu, lokale Deckungen auf das Niveau des Mastervertrages generell oder in Einzelfällen anzuheben. Dies kann sowohl für integrierte als auch für koordinierte Programme vereinbart werden. Als weitere wesentliche Klauseln haben sich etabliert:

20.4.4.1 „Step Down/Drop Down“-, auch Summenausschöpfungsklausel

Hierdurch wird die lokale Deckungssumme aus dem Mastervertrag heraus aufgefüllt, wenn diese durch Schäden bereits unterjährig ausgeschöpft wird.

Diese Regelungen sind eher in Haftpflicht-IVP üblich, als in der Sachversicherung, und greifen ein, wenn die Versicherungssumme der Lokalpolice erschöpft ist. In diesen Fällen steht dann die Versicherungssumme des Mastervertrages für weitere lokale Schäden von Grund auf zur Verfügung, wobei gelegentlich ein etwas höherer Selbstbehalt zur Anwendung kommt, als jener, der in der Lokalpolice vereinbart wurde.

20.4.4.2 „Reverse DIC“-Klausel

Durch die „Reverse Difference in Conditions“-Klausel wird erreicht, dass lokale Sonderdeckungen, die im deutschen Mastervertrag nicht zur Verfügung stehen, technisch in den Mastervertrag einbezogen werden und insoweit darüber auch höhere Deckungssummen aus dem Mastervertrag bereitgestellt werden, als es die jeweilige Lokalpolice vorsieht (ein Beispiel für eine solche Klausel bei Brühwiler 1994, S. 186, Rn. 324.13). Dies gilt immer nur für das betreffende Land und kann beispielsweise dann erforderlich sein, wenn in einem der durch den Mastervertrag versicherten Länder ein besonderes Geschäft betrieben wird, welches sich in seinem Risiko deutlich vom Kerngeschäft der übrigen Standorte unterscheidet.

Die „Reverse DIC“ ist im Gegensatz zu anderen Klauseln aber nicht zwangsläufig Bestandteil eines IVP, da sie in der Regel nur für einzelne Gesellschaften individuell vereinbart wird. In der juristischen Literatur wird sie deutlich seltener erwähnt als andere Vertragsklauseln (erwähnt wird diese Klausel zum Beispiel bei Schürpf 1984, S. 235 und 240; vgl. Brühwiler 1994, S. 185 f., Rn. 324.13; Mächler-Erne 2000, S. 153 und 163; vgl. Mazzanauer 2008, 19 f.; vgl. Nickel 2014, Ziff. 6868, S. 2), auch weil sie deutlich seltener vereinbart wird, als andere hier genannte Klauseln. Für Haftpflichtversicherungsprogramme, deren Ausgestaltung stärker als im Sachversicherungssektor durch nationales Recht geprägt ist, erweist sich diese Klausel häufiger als praxisrelevant.

20.4.4.3 „Extended Reverse DIC“-Klausel

Über diese noch seltenere Erweiterung im Mastervertrag wird eine lokale Sonderdeckung auch allen anderen Ländern bereitgestellt. Darüber kann eine maximale Konsistenz im IVP hergestellt werden – quasi eine weltweite „Best-of“-Deckung. Obwohl aus Sicht des Versicherungsnehmers wünschenswert, wird diese Klausel durch Versicherer üblicherweise nicht akzeptiert.

20.4.5 Spezifische Anforderungen

Hinsichtlich der Verwendung von Verknüpfungsklauseln sind verschiedene, spezifische Herausforderungen zu berücksichtigen:

20.4.5.1 Compliance

Auch wenn die Verknüpfungsklauseln suggerieren, dass über deren Vereinbarung ohne weiteres eine weltweit konsistente Absicherung gewährleistet werden kann, macht die Komplexität internationaler Regelwerke (etwa Vertragsrecht, Aufsichtsrecht und Steuerrecht) eine differenziertere Betrachtung notwendig: Bei gut 190 Ländern, in denen Versicherungsprogramme abgebildet werden können, existieren über 250 verschiedene Bestimmungen zur Versicherungsaufsicht oder zur Behandlung der Versicherungssteuer.

In den sogenannten „Non-admitted“-Ländern ist das Bereitstellen weitergehenden Versicherungsschutzes als über die begrenzte lokale Deckung unter Zuhilfenahme von Verknüpfungsklauseln im Zweifel nicht zulässig. Die gewünschten Deckungen müssten dann, wie oben erwähnt, über „Stand alone“-Deckungen abgebildet werden. Zu den Verbotsländern gehören zum Beispiel die BRICS-Staaten (Brasilien, Russland, Indien, China, Südafrika) oder auch die Schweiz.

Im Zusammenspiel von Lokalpolicien und Differenzdeckungen kann es je nach ausländischer Jurisdiktion bei der Regulierung ausländischer Schadenfälle zu Komplikationen kommen. Um dem zu begegnen, wird übergreifender Versicherungsschutz teilweise über die bereits angesprochene, sogenannte Wertverlustklausel (bekannt auch als Financial-Interest-Cover/FinC) abgebildet. Hiermit wird das inländische Interesse der Muttergesellschaft am Werterhalt der Auslandsbeteiligungen versichert. Im Ergebnis entspricht dies einer Absicherung finanzieller Eigenschäden. Die Versicherung des finanziellen Verlustes ist in Deutschland im Nr. 16 g) Anh. 1 zum Versicherungsaufsichtsgesetz als dort sogenannter Wertverlust zugelassen.

Bei den Verknüpfungsklauseln oder auch bei Vereinbarung einer Wertverlustklausel bestehen bei sorgfältiger vertraglicher Gestaltung kaum Bedenken, dass diese mit deutschem Recht nicht vereinbar sind. Für die „Non-admitted“-Länder kann dies jedoch nicht immer mit Sicherheit gesagt werden – besonders vor dem Hintergrund teilweiser ungenügender Transparenz im lokalen Aufsichtsrecht oder zum Teil nicht konsistenter behördlicher Praxis.

Im Schadenfall kann zum Beispiel die sonst übliche Regulierung direkt an die Tochtergesellschaft unzulässig sein. Davon abweichende Zahlungsvarianten können wiederum steuerliche Implikationen auslösen, was daher eingehender Beratung bedarf und mit Blick auf das präferierte Ergebnis sorgfältig abzuwegen ist. Diese verbleibende Ungewissheit erstreckt sich schließlich auch auf andere steuerrechtliche Sachverhalte. Versicherungssteuern und Abgaben sind je Land korrekt zu berechnen und vor Ort abzuführen. Auch die Frage nach dem richtigen Steuerschuldner ist nicht immer einheitlich und rechtssicher zu beantworten.

Ohne vertiefend auf steuerliche Gesichtspunkte bei der Gestaltung eines IVP einzugehen, zumindest ein paar grundsätzliche Hinweise: Nach dem Urteil des EuGH in der Rechtssache „Kvaerner“ richte sich die Steuerschuld grundsätzlich nach der Risikobelegenheit und es komme damit der lokale Versicherungssteuersatz in dem Land der Risikobelegenheit zur Anwendung. Genauer heißt es dort: „Ein Mitgliedstaat kann Versicherungssteuer auf eine Prämie verlangen, die sich auf die Versicherung einer

Tochtergesellschaft bezieht, die in diesem Staat registriert wurde, und zwar auch dann, wenn die Prämie in einem anderen Land durch die Muttergesellschaft beglichen wurde.“ (EUGH Urteil C-191/99 vom 14.06.2001)

In der Praxis kommt es jedoch immer wieder vor, dass der für das Ausland allokierte Prämienanteil nicht risiko- und damit sachgerecht ist, da zum Beispiel Verknüpfungsklauseln aus Masterdeckungen nicht berücksichtigt wurden. In anderen Fällen werden lokal entweder gar keine Steuern oder aber mit dem dort nicht anwendbaren deutschen Steuersatz abgeführt. Als Konsequenz derartiger Unsicherheiten können zum Teil hohe Nachzahlungsverpflichtungen drohen, insbesondere dann, wenn die Steuerpraxis über viele Jahre nicht korrekt war.

Die Versicherer als Anbieter der IVP haben hierzu (aus Sicht der versicherungsnehmenden Industrie leider) keine einheitliche Sichtweise. Daher müssen Unternehmen häufig selbst entscheiden, ob sie eine Absicherung von Tochterunternehmen in den sogenannten Verbotsländern über eine „DIC/DIL“- oder FINC-Deckung vornehmen möchten. Zudem kann es für dasselbe Tochterunternehmen im Ausland in verschiedenen Versicherungssparten verschiedene Lösungen geben. Denn die unter Compliance-Gesichtspunkten bedeutsame Risikobelegenheit kann von Sparte zu Sparte sehr unterschiedlich sein – leicht nachvollziehbar etwa in den Unterschieden zwischen Haftpflicht-, Sach- und Transportversicherungsprogrammen.

20.4.5.2 Länder- und Spartenbesonderheiten

Wie wichtig lokale Expertise bei der Konzeption eines IVP ist, wird zudem deutlich, wenn man anhand nur einiger Beispiele aufzeigt, mit welchen besonderen Herausforderungen versicherungsnehmende Unternehmen im Ausland konfrontiert werden können. Die Berücksichtigung dieser Herausforderungen und eine nahtlose Integration entsprechender Lösungen in einem IVP kann in der Praxis sehr anspruchsvoll sein – sowohl deckungstechnisch als auch administrativ:

- „Cash before cover“-Länder: In manchen Ländern darf Deckung erst dann gewährt werden, wenn die Prämie entrichtet ist, das heißt, die entsprechende Prämie muss vor Beginn des Versicherungsvertrags alloziert und bezahlt worden sein (Beispiele: Japan und Russland). Dies stellt häufig eine große administrative Herausforderung dar, nicht nur wenn eine Einigung zwischen Versicherer und Kunde erst spät erfolgt.
- Tarifmärkte: Preise und Deckungsumfang in anderen Ländern werden lokal strikt vorgegeben, sind kaum verhandelbar und im Ergebnis dann zu teuer und im Umfang ungenügend (zum Beispiel Brasilien und Japan). Entsprechende Deckungslücken müssen durch den Mastervertrag im Rahmen der DIC-/DIL-Deckung oder durch eine Wertverlustklausel ausgeglichen werden.
- Staatliche Poolls Lösungen: In manchen Ländern gibt es für bestimmte Risiken Versicherungen mit Pflichtprämienanteilen für staatliche Versicherungspools. Beispiele hierfür sind die Terrordeckungen GAREAT in Frankreich (Gestion de l'Assurance et de la Réassurance des) in den USA.

- „Foreign Account Tax Compliance Act“ (FATCA): Dieses im Jahr 2010 in Kraft getretene US-Gesetz sieht weitreichende Dokumentierungspflichten zum Nachweis der ordnungsgemäßen Abführung von Versicherungssteuern für Auslandsgesellschaften in den USA vor.
- „Boiler & Machinery“-Anforderungen: Schließlich sind in einigen Ländern Inspektionen bei benannten Maschinen und Kesseln gesetzlich vorgeschrieben. Diese Inspektionen können gemeinsam mit der entsprechenden Versicherungsdeckung optional in lokale Deckungen eingeschlossen werden (vornehmlich in den USA und UK).

20.4.5.3 Administration

Selbst wenn man mit entsprechender Beratung und daraus resultierendem Aufwand über die Zeit für die Mehrzahl der vorgenannten Themen konzeptionelle Lösungen gefunden hat, hängt der Erfolg eines IVP vor allem von der konsequenten Umsetzung und einer fortlaufend effizienten Administration ab. Die Komplettierung, Platzierung und Implementierung anspruchsvoller und komplexer Programme ist maßgeblich vom Zusammenspiel zwischen Versicherungsnehmer, Versicherern und dem Netzwerkmakler abhängig. Eine effiziente und gut eingespielte Netzwerkkoordination, systembasierte Instruktionen und eine gute und wirksame Kommunikation zwischen allen Parteien bilden die Grundvoraussetzungen für zuverlässigen und korrekten Informations- und Datenaustausch, wodurch das Fehlerrisiko bei der Handhabung und vor allem auch im Schadenfall signifikant reduziert wird. Der Auswahl professioneller und international erfahrener Versicherer, Makler und Servicepartner kommt unter diesem „administrativen“ Gesichtspunkt eine außerordentliche Bedeutung zu.

20.4.5.4 Politische Herausforderungen: „Brexit“, Sanktionen

Weitere Herausforderungen für IVP können sich manchmal sehr rasch und schwer vorhersehbar aus Entwicklungen ergeben. So gibt es im Zuge des sogenannten „Brexit“, also des Austritts Großbritanniens aus der Europäischen Union, nach wie vor viele Fragen, die nicht abschließend und rechtssicher beantwortet werden können. Der Vorsorge- und Beratungsbedarf bei Unternehmen für ihre internationalen Versicherungsrisiken bleibt dabei hoch.

Auch stehen die Programmversicherer – und damit auch die Versicherungsnehmer – vor großen Herausforderungen, wenn, wie im November 2018, US-Sanktionen gegen den Iran (wieder) in Kraft treten. Zumal sich die Wirksamkeit von Sanktionen unterschiedlich darstellt, je nachdem, ob man mit einem europäischen Versicherer zusammenarbeitet, der mit seinem Geschäft eine nur geringe US-Exponierung aufweist, oder aber mit einem US-Versicherer bzw. dessen deutscher Niederlassung. Die aktualisierte sogenannte „Blocking Regulation“ der EU untersagt unter Androhung von Bußgeldern nun auch europäischen Versicherern, die US-Sanktionen zu befolgen. Versicherer können dadurch im Ergebnis nicht mehr ohne Weiteres Sanktionsklauseln vereinbaren bzw. diese im Schadenfall exekutieren. Andererseits kann ein Verstoß gegen die US-Sanktionen zumindest für US-Versicherer, aber auch für die US-Niederlassungen europäischer Versicherer deren Li-

zenz gefährden und damit die Stabilität von IVP tangieren. Für alle Beteiligten ein Dilemma, was gut durchdachte und sorgfältig ausbalancierte Einzelfallentscheidungen erforderlich macht.

20.5 Schlussbemerkung und Ausblick

Um dem Anspruch möglichst weitreichender Einhaltung der Compliance-Anforderungen an ein IVP zu genügen, bedarf es immer wieder sorgfältiger Überprüfungen. Aufwand und Kosten hierfür sind hoch. Hundertprozentige Sicherheit gibt es dabei nicht, da die zugrunde liegenden (jeweils nationalen) Regelungen häufig miteinander konkurrieren. Trotzdem dürfen die in Deutschland verfügbaren IVP im weltweiten Vergleich als sehr individuelle und anspruchsvolle Lösungen bezeichnet werden.

Im Zusammenspiel zwischen Mastervertrag und lokalen Policen werden die wesentlichen risikoseitigen, versicherungstechnischen und betriebswirtschaftlichen Vorteile eines integrierten IVP schnell deutlich, weshalb diese Variante im deutschen Markt nach wie vor am weitesten verbreitet ist. Sie gewährleistet:

- Sicherstellung weltweit möglichst konsistenten Versicherungsschutzes für die gesamte Unternehmensgruppe;
- zentrale Kontrolle und Steuerung durch die Muttergesellschaft und damit stringente Umsetzung der Risikomanagement-Strategie;
- Bereitstellung hoher Kapazitäten für die gesamte Gruppe;
- Optimierung der Versicherungskosten durch die Programmstruktur als solches (Mastervertrag mit DIC/DIL macht weniger Kapazität erforderlich) und die quasi-weltweite Bündelung des Versicherungseinkaufs (Skaleneffekte);
- weltweite Schadenübersicht als wichtige Information für das Risikomanagement sowie die Erneuerungsverhandlungen mit den Versicherern;
- zentrale und lokale Administration und Schadenregulierung unter Berücksichtigung lokaler Haftungsnormen, länderspezifischer Deckungsbesonderheiten und Rechtsprechung;
- Berücksichtigung von „non admitted“-Vorschriften und weitreichende regelkonforme Lösungsoptionen für Verbotsländer durch das Zusammenspiel lokaler Deckungen mit adäquaten Verknüpfungsklauseln.

Dennoch dürfen abschließend zwei wesentliche Bereiche nicht unerwähnt bleiben, deren Weiterentwicklung unter vielerlei Gesichtspunkten dringend erforderlich ist – besonders, um künftig für alle Beteiligten mehr Rechtssicherheit und Effizienz zu schaffen:

Dies sind zum einen Automatisierung und Digitalisierung: Die Systeme international operierender Versicherer und Makler sind in den vergangenen Jahren zwar beständig leistungsfähiger und zuverlässiger geworden. Das wenig koordinierte Vorantreiben heterogener Strukturen muss jedoch baldmöglichst dem Streben nach einheitlichen technischen Standards, Prozessen und Schnittstellen weichen, um die Versicherungsbranche und ihre wertvollen Lösungen auch technologisch und kostenseitig wettbewerbsfähig zu halten.

Der zweite wichtige Bereich ist die möglichst weltweite Harmonisierung: Zwar ist die beschriebene Komplexität der weltweiten versicherungsrelevanten Regelwerke im Aufsichtsrecht, im Vertragsrecht und im Steuerrecht häufig auch politisch, das heißt protektionistisch motiviert. Doch trotzdem muss der Versuch unternommen werden, im Interesse aller Beteiligten eine weltweit ausbalancierte Harmonisierung herbeizuführen. Der GVNW (Gesamtverband der versicherungsnehmenden Wirtschaft), die Interessenvertretung der deutschen, industriellen Versicherungsnehmer, hat in dieser Sache einen ersten Vorstoß unternommen. Als Mitglied der IFRIMA (International Federation of Risk and Insurance Management Associations) und mit dieser als Vehikel wurden erste konstruktive Gespräche mit der IAIS (International Association of Insurance Supervisors) geführt. Die IAIS ist sicherlich ein möglicher Adressat, sofern es um die weltweite Standardisierung nationalen Versicherungsaufsichtsrechts geht. Im nächsten Schritt müssen jedoch weitere interessierte Parteien als Sponsoren für dieses Anliegen gewonnen werden und weltweit muss entsprechende Überzeugungsarbeit (zum Beispiel bei nationalen Aufsichtsbehörden) geleistet werden. Es liegt insofern auf der Hand, dass es hier noch viel Zeit, Geduld und Beharrlichkeit braucht, um die gewünschte Harmonisierung auf den Weg zu bringen.

Literatur

- Armbrüster, C. (2008). Versicherung des Finanzinteresses in internationalen Versicherungsprogrammen. *VersR*, 2008(19).
- Bähr, G., & Püttgen, F. (2008). Financial Interest Cover; Zeitgemäße Ausgestaltung von internationalen Versicherungsprogramme. *VW*, 2008(13), 1078 ff.
- Basedow, J., & Scherpe, J. (2005). Das internationale Versicherungsvertragsrecht und „Rom I“. In S. Lorenz et al. (Hrsg.), *Festschrift für Andreas Heldrich zum 70. Geburtstag*. München: C.H. Beck.
- Bialowons, A., & Kerst, A. (2011). Rahmenbedingungen bei der Gestaltung von internationalen Versicherungsprogramme; Die non-admitted-Problematik. *r+s*, 2011(8), 317 ff.
- Brühwiler, B. (1994). *Internationale Industriever sicherung; Risk-Management, Unternehmensführung, Erfolgsstrategien*. Karlsruhe: Versicherungswirtschaft.
- Farny, D. (1984). Auslandsaktivitäten deutscher Versicherungsunternehmen. *VW*, 1984(1), 31 ff.
- Kasper, A. (2008). FIC-Konzept kontrovers diskutiert; Versicherung des finanziellen Interesses. *contact*, 2008(10), 2.
- Koch, R. (2009). Kollisions- und versicherungsrechtliche Probleme bei internationalen D&O-Haftungsfällen. *VersR*, 2009(4), 141.
- Langheid, T., & Grote, J. (2008). Droht die Rote Karte? – Internationale Versicherungsprogramme und die Versicherung des finanziellen Interesses. *Versicherungswirtschaft*, 2008(8), 630 ff. und 1510.
- Laupichler, A., & Post, J. (2008). Chancen verwerten statt Eigentore zu schießen! In der jüngst kontrovers geführten Debatte über die Versicherung des finanziellen Interesses vorgebrachte Scheinargumente helfen nicht weiter. *VW*, 2008(11), 914 f.
- Mächler-Erne, M. (2000). Internationale Versicherungsverträge – Formen und Inhalt. In F. Reichert-Facilides & A. Schnyder (Hrsg.), *Versicherungsrecht in Europa – Kernperspektiven am Ende des 20. Jahrhunderts*. Basel/Genf/München: Helbing & Lichtenhahn.
- Mahnke, A. (2008). Internationale Anforderungen an die D&O Versicherung. *Handelsblatt Veranstaltungen, Newsletter*, 2008(3), 8 ff.

- Mazenauer, H. (2008). Globalisierung befähigt Internationale Programme – Compliance und Corporate Governance nötigen zur Weiterentwicklung – Neueste Lösungen bewältigen auch lizenzi- und steuerrechtliche Hürden. *VW, 2008(1)*, 19 ff.
- Nickel, F. (2014). I. Ziff. 4.4 PHB: Aus- und Einbaukosten – Teil Versicherungsschutz. In H. J. Kullmann et al. (Hrsg.), *Produzentenhaftung*. Berlin: Erich Schmidt.
- Quitzau, et al. (2018). Schifffahrt in Zeiten des digitalen Wandels. Strategie 2030. HWI/Beerenberg, Hamburg 2018 ff.
- Schürpf, W. (1984). Internationale Risiken verlangen internationale Versicherungslösungen. In M. Haller & W. Ackermann (Hrsg.), *Internationalität der Versicherung – Festgabe für Marcel Grossmann zum 80. Geburtstag*. St. Gallen: Institut für Versicherungswirtschaft an der Hochschule St. Gallen.
- Strnad, M. (2007). Neue Ausgestaltung internationaler Versicherungsprogramme; Gründe, Formen und Rückschlüsse auf die grenzüberschreitende Schadenabwicklung. *HAVE/REAS, 2007(4)*, 345 ff.
- Strnad, M. (2008). Klassenbester oder Spielverderber? Neue Wege in der Ausgestaltung, 1263, 1266, 1270. Versicherungsprogramme. *VW, 2008*, 15 ff.
- Strnad, M. (2009). International Insurance Programs – Legal Frictions and Solutions. *IICJ, 2009*.
- UNCTAD. (2002). World Investment Report 2002.
- Wolterec, R. (1988). Auslandsgeschäft. In D. Farny et al. (Hrsg.), *Handwörterbuch der Versicherungswirtschaft HdV*. Karlsruhe: Versicherungswirtschaft.

Rüdiger Auras leitet seit 2018 den Bereich Strategic Account Management bei Aon Commercial Risk Solutions in Deutschland. Er hat über 20 Jahre Erfahrung im Underwriting internationaler Versicherungsprogramme bei führenden Industriever sicherern im In- und Ausland, zuletzt als Head of Property, Marine & Engineering Lines bei Zurich Global Corporate, Germany. Bevor er in 2018 zu Aon wechselte, war er über sechs Jahre Geschäftsführer des Gesamtverbands der versicherungnehmenden Wirtschaft e. V.

Michael Dehm leitet seit Juli 2019 die strategischen und kommerziellen Aktivitäten des Bereichs „Global Benefits“ im Segment „Aon Health Solutions“. Mit nahezu 25 Jahren in der Versicherungsindustrie hat der zugelassene Rechtsanwalt bis heute eine Vielzahl von Positionen im Seniormanagement sowohl bei internationalen Versicherungsunternehmen wie auch bei Großmaklern begleitet. Der Schwerpunkt seiner Tätigkeit lag dabei stets in der Bereitstellung weltweiter Versicherungslösungen und entsprechender Beratungs- sowie Serviceleistungen für multinational operierende Großunternehmen.



Cyber

21

Cyber-Risiken, eine wachsende Bedrohung

Andreas Walz, Jörg Klemens und Romina Röpke

Zusammenfassung

Im Zuge der Digitalisierung und der zunehmenden Vernetzung der Weltwirtschaft werden Unternehmen mit neuen Risiken konfrontiert. Hierzu gehören insbesondere auch Cyber-Risiken. Besonders Malware, Social Engineering und DDoS-Attacken spielen in diesem Kontext eine wichtige Rolle. Die Angreifer nutzen hierzu verschiedene Methoden, um Daten zu stehlen, zu manipulieren oder zu zerstören, so dass Unternehmen hohe Schäden durch Betriebsunterbrechungen oder auch Haftungsschäden gegenüber Dritten erleiden. Kleine, mittlere und große Unternehmen jeglicher Branchen müssen sich mit diesem Thema auseinandersetzen und die Schwachstellen in ihrem Unternehmen identifizieren. Ein wirksames Risikomanagement kann dabei helfen, Risiken zu identifizieren und geeignete Maßnahmen zu entwickeln. Versicherungslösungen können einen sinnvollen und wichtigen Baustein zum Schutz vor Cyber-Risiken darstellen. Der Markt für Cyber-Policen wächst stetig und Versicherungsunternehmen bieten ihren Kunden, neben der rein finanziellen Absicherung, immer mehr Service-Leistungen, die den Unternehmen helfen, mit diesen neuartigen Risiken umzugehen.

A. Walz (✉) · J. Klemens
Talanx Group, Hannover, Deutschland
E-Mail: andreas.walz@hdi.de; Joerg.Klemens@hdi.de

R. Röpke
TH Köln, Institut für Versicherungswesen, Köln, Deutschland
E-Mail: ro.roepke@gmail.com

21.1 Einleitung

21.1.1 Bedeutung von Cyber-Risiken

Die zunehmende Digitalisierung schafft neue Möglichkeiten in allen Branchen und Geschäftsbereichen. Heute spielen Informationstechnologien nicht nur für IT-Unternehmen eine wichtige Rolle, sondern auch kleine, mittelständische und große Unternehmen nutzen modernste Technik, um Prozesse effizienter zu gestalten, neue Geschäftsmodelle zu entwickeln oder um in neue Märkte einzutreten. Die Vernetzung geht über nationalen Grenzen hinaus und ermöglicht die Veränderung, Verkürzung und Verbesserung von Produktions- und Wirtschaftsabläufen. Aktuelle Trends, wie Industrie 4.0 und Internet of Things (IoT), basieren auf einem Konzept der Verknüpfung von digitaler und realer Welt. Der digitale Fortschritt verändert damit nicht nur die Geschäftswelt, sondern hat ebenfalls Auswirkungen auf eine Vielzahl privater Lebensbereiche.

Durch die zunehmende Vernetzung und die damit einhergehende Abhängigkeit von Informationstechnologien setzen sich Unternehmen und Privatpersonen neuen Gefahren aus. Cyber-Kriminelle nutzen Schwachstellen wie Systeme, Hardware oder Prozesse, aber auch Mitarbeiter oder andere Menschen, um sich Zugriff zu Systemen zu verschaffen und an die Daten von Privatpersonen oder Unternehmen zu gelangen. Datendiebstahl, -missbrauch, -manipulation oder -zerstörung sind die Folgen von Cyber-Attacken. Die Vorfälle von Cyber-Attacken häufen sich, so dass sieben von zehn Unternehmen bestätigen, bereits Opfer von Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden zu sein (vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. 2018, S. 14). Die Motivationen der Angreifer sind dabei so unterschiedlich, wie ihre Herangehensweisen. Die in den Medien genannten Ziele sind nicht nur IT-Unternehmen wie Facebook, Google oder Amazon, sondern auch die NATO, das deutsche Luft- und Raumfahrtzentrum und der Bundestag. Besonders viel Aufsehen erregten insbesondere Schadprogramme wie „WannaCry“ und „Petya/NotPetya“ (vgl. Allianz Global Corporate & Specialty SE 2019, S. 6).

Cyber-Attacken können jeden treffen, doch besonders kleine und mittelständische Unternehmen sind sich der Gefahr und der damit verbundenen Schadenpotenziale häufig nicht bewusst. Wird ein kleines Unternehmen von Kriminellen ins Visier genommen, so kann zum Beispiel eine, aus einem Angriff resultierende, Betriebsunterbrechung eine Bedrohung für die Existenz des Unternehmens darstellen (vgl. Allianz Global Corporate & Specialty SE 2019, S. 14). Angriffe auf große Unternehmen scheinen aufgrund ihres Kapitals, der Unternehmensgeheimnisse und der immensen Mengen an Daten lukrativer, jedoch sind die Informationssysteme dieser Unternehmen durch eine bessere IT-Infrastruktur meist besser geschützt.

In einem sich ständig wandelnden Umfeld verändern sich auch die damit einhergehenden Risiken. Nicht grundlos werden Cyber-Risiken laut dem „Allianz Risk Barometer – Top Business Risks for 2019“ für Unternehmen im Jahr 2019 als zweitwichtigstes Risiko eingestuft (vgl. Allianz Global Corporate & Specialty SE 2019, S. 4). Daraus ergeben sich

folgende Fragen: Wie können sich Unternehmen vor solchen Risiken schützen? Welche Maßnahmen können ergriffen werden, um das Auftreten von Cyber-Attacken zu verhindern? Wie gehen Unternehmen im Notfall mit einem solchen Angriff und den damit verbundenen Schäden um? Und welche Möglichkeiten der Absicherungen gibt es?

21.1.2 Begriffsabgrenzung

Der Begriff „Cyber“ stammt ab von dem Wort Kybernetik (englisch: „cybernetics“), welches „Wissenschaft von den Steuerungs- und Regelungsvorgängen“ bedeutet. Laut Duden beschreibt „Cyber“ ein Wortbildungselement mit der Bedeutung „die von Computern erzeugte virtuelle Scheinwelt betreffend“ (Dudenredaktion o. J.), zum Beispiel Cyberspace. Das Cambridge Dictionary beschreibt das Präfix „Cyber“ mit „involving, using, or relating to computers, especially the internet“ (Cambridge Dictionary 2020) und das Oxford Dictionary als „connected with electronic communication networks, especially the internet“ (Oxford Advanced Learner’s Dictionaries o. J.).

Die Definitionen des Begriffes „Cyber“ häufen sich in der Literatur, und auch wenn die Definitionen Unterschiede aufweisen, so gibt es doch einen Konsens: „Cyber“ wird als Präfix verwendet und bezieht sich auf das Internet, eine virtuelle Realität oder auf eine von Computern erzeugte Umgebung.

Für dieses Kapitel wichtige Begriffe sind unter anderem „Cyber-Risiko“ sowie „Cyber-Sicherheit“. Letzterer wird oft mit den Begriffen „IT“ und „Informationssicherheit“ synonym verwendet, jedoch beschreibt „Cyber“ weitaus mehr, als diese Begriffe abdecken. Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) beschäftigt sich IT-Sicherheit „.... an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung“ (Bundesamt für Sicherheit in der Informationstechnik 2019b). „Informationssicherheit“ hingegen hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein (vgl. Bundesamt für Sicherheit in der Informationstechnik 2019b). „Cyber-Sicherheit“ geht weiter darüber hinaus und bezieht alle Aspekte der IT- und Informationssicherheit mit ein und weitet diese auf den gesamten Cyber-Raum aus. „Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein“ (Bundesamt für Sicherheit in der Informationstechnik 2019b).

Das „Cyber-Risiko“ ist somit eine „aus der Unvorhersehbarkeit der Zukunft resultierendes, durch (zufällige) Störungen verursachte Möglichkeit, von geplanten Zielwerten abzuweichen“ (RiskNET), bezogen auf den „Cyber-Raum“.

21.2 Cyber-Risiken

21.2.1 Schäden/Schadenpotenziale

Schäden durch Cyber-Risiken sind so vielseitig wie die Gründe ihrer Entstehung. Dabei wird das Ausmaß eines solchen Schadens durch die Schadenhöhe definiert, welche direkte Kosten finanzieller Art beinhaltet, sowie durch die Folgen von Reputationsschäden. Letztere lassen sich nur schwer beziffern, weswegen die Schadenhöhe aufgrund von Cyber-Risiken häufig nur auf Schätzungen beruht (vgl. Bundesamt für Sicherheit in der Informationstechnik 2019a). Die Höhe der Schäden, die durch Wirtschaftsspionage, Sabotage, und Diebstahl verursacht werden, reicht von Kleinstbeträgen bis hin zu Schäden im Milliardenbereich. Laut einer Studie des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e. V. (kurz Bitkom) zum Thema „Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie“ im Jahre 2018 lag der Schaden durch die Folgen digitaler Wirtschaftsspionage, Sabotage und Datendiebstahls in Deutschland nach konservativen Berechnungen bei rund 43,4 Milliarden Euro (vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. 2018, S. 25).

Die Schadenpotenziale betreffen nicht nur die Unternehmen an sich, sondern durch Fehlverhalten oder Cyber-Attacken können auch für Dritte Schäden entstehen. Somit muss zwischen den **Eigenschäden** des Unternehmens und dem finanziellen Anspruch Dritter, den sogenannten **Drittschäden**, differenziert werden.

Eigenschäden (First Party Losses)

Kosten durch **Betriebsunterbrechungen** haben für Unternehmen schwerwiegende Konsequenzen. Laut dem „Allianz Risk Barometer“ für das Jahr 2019 gelten für 69 Prozent der Befragten Betriebsunterbrechungen und die damit verbundenen Umsatzeinbußen, als Hauptursache für wirtschaftliche Schäden hinsichtlich Cyber-Risiken (vgl. Allianz Global Corporate & Specialty SE 2019, S. 14). In Deutschland sind in den letzten zwei Jahren laut Bitkom-Studie 6,7 Milliarden Euro Schaden durch Umsatzeinbußen in Folge eines Ausfalls oder einer Störung der Betriebsabläufe entstanden (vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. 2018, S. 25). Besonders Cyber-Angriffe sind hier von Bedeutung. Immerhin gaben 28 Prozent der Industrieunternehmen an, bereits sabotiert worden zu sein. Da nicht jede Cyber-Attacke auch als solche erkannt wird, kann der dadurch verursachte Schaden nur schwer ermittelt werden (vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. 2018, S. 15).

Reputationsschäden werden von 55 Prozent der Befragten als größter Kostenverursacher wahrgenommen (vgl. Allianz Global Corporate & Specialty SE 2019, S. 14). Und obwohl Imageschäden bei Kunden und Lieferanten, und das damit verbundene Abwandern von Kunden, nur sehr schwer schätzbar sind, beläuft sich der Schaden aufgrund von Reputationsverlust bzw. negativer Medienberichterstattung in Deutschland auf rund 8,8 Milliarden Euro allein in den letzten zwei Jahren (vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. 2018, S. 25). Ca. 41 Prozent der

Unternehmen, die Opfer von Wirtschaftsspionage, Sabotage oder Datendiebstahl wurden, berichteten von Imageschäden bei Kunden und Lieferanten (vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. 2018, S. 22).

Die Bandbreite an **physischen Schäden bzw. Sachschäden** reicht vom Diebstahl technischer Geräte bis hin zu defekten Maschinen, zerstörten Rechenzentren und beschädigten Datenträgern. 32 Prozent gaben an, dass ihnen Geräte wie Notebooks oder Smartphones entwendet wurden (vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. 2018, S. 15).

Für 29 Prozent der Befragten stellen Kosten für die **Wiederherstellung von Daten** eine bedeutende finanzielle Belastung dar (vgl. Allianz 2019, S. 14). Selbst wenn es gelingt die Daten wiederherzustellen, erzeugt ein Angriff hohe Kosten. Durch die Komplexität der Angriffe sind hohe Aufwendungen hinsichtlich der **Aufklärung der Fälle** (zum Beispiel **IT-Forensik**) notwendig. Eine **juristische Analyse** des Vorfallen sowie mögliche **Gerichtskosten** sind ebenfalls Kostentreiber (vgl. Flagmeier und Heidemann 2018, S. 20). Die Kosten für Ermittlungen wurden auf ca. 5,7 Milliarden Euro und Kosten für Rechtsstreitigkeiten auf ca. 3,7 Milliarden Euro allein für die letzten beiden Jahre innerhalb Deutschlands geschätzt (vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. 2018, S. 25). Nicht zu unterschätzen sind auch die **Kosten für Notfallmaßnahmen**, zum Beispiel für die Benachrichtigung der Kunden, Lieferanten und Behörden oder für den Einsatz eines PR-Beraters (vgl. Flagmeier und Heidemann 2018, S. 38–39). Aufgrund des rechtlichen Hintergrundes zum Thema Datenschutz fallen für einen Großteil der Unternehmen (ca. 40 Prozent der befragten Unternehmen) nach einem Angriff zusätzliche Kosten für **datenschutzrechtliche Maßnahmen** an (vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. 2018, S. 22). Lösegeldzahlungen in Folge einer **Erpressung** durch „Ransomware“ (vgl. Abschn. 21.2.4.1) verursachten in den letzten zwei Jahren 300 Millionen Euro Schaden (Tendenz fallend, da Unternehmen im Falle einer Erpressung immer seltener der Lösegeldforderung nachgehen (vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medi-en e. V. 2018, S. 25)).

Drittschäden (Third Party Losses)

Eine weitreichende Folge von Datenverlusten sind die monetären Ansprüche Dritter. Damit das Unternehmen haftbar gemacht werden kann, muss eine Handlung oder Unterlassung des Unternehmens den Schaden überhaupt ermöglicht haben. Besonders die Frage, ob das Unternehmen haftbar für die Schäden Dritter ist, ist oft unklar. Der Cyber-Raum geht über nationale Grenzen hinaus, doch rechtliche Ansprüche basieren auf der jeweiligen nationalen Gesetzgebung. Liegt eine **datenschutzbezogene Pflicht- und Vertraulichkeitsverletzung** vor, so stellen sich weitere Fragen. Handelt es sich um eine Eigentumsverletzung oder ist durch den Datenverlust ein echter Vermögensschaden entstanden? Wie hoch ist der entstandene Schaden (ausgedrückt als monetärer Wert)? Können durch einen Datenverlust geschädigte Personen oder Unternehmen die Kosten für Datenwiederherstellung, Reputationsverluste bei Kunden oder Kosten aus der Beeinträchtigung oder Verwehrung des berechtigten Zugangs geltend machen? (vgl. Flagmeier und Heidemann 2018, S. 39–40)

Neben monetären Schäden kann auch Gefahr für Leib und Leben bestehen. Das durch Cyber-Kriminelle verursachte Entgleisen eines Zuges kann viele Menschen das Leben kosten. Und auch das Entwenden von Daten kann zum Beispiel im Falle von Stalking das leibliche Wohl von Menschen negativ beeinflussen.

21.2.2 Bedrohungspotenziale

Cyber-Risiken (vgl. Abb. 21.1) beschränken sich nicht nur auf die Angriffe von Cyber-Kriminellen, sondern umfassen auch **nicht-kriminelle Ursachen**. Höhere Gewalt in Form von Naturkatastrophen, Überschwemmungen, Erdbeben oder Stromausfällen kann zum Verlust von Daten führen, wenn die Technik in den Rechenzentren zerstört oder beschädigt wird. Oft ist es auch menschliches Versagen oder Fehlverhalten, welches zu großen Schäden führt. Die versehentliche Veröffentlichung sensibler Daten oder eine falsche Adressierung bei Post- oder E-Mail-Verkehr kann unterschiedlichste negative Folgen haben. Zu den Ursachen von Cyber-Risiken gehört nicht nur das menschliche, sondern auch das technische Versagen. Fehlerhafte Soft- oder Hardware kann Datenverluste nach sich ziehen. Durch einen Kurzschluss oder das Überhitzen der Technik können Datenspeicher beschädigt werden und so Daten unwiederbringlich zerstört werden (vgl. Brokamp 2017, S. 40).

Auch wenn nicht hinter jedem Datenverlust eine kriminelle Absicht steht, so sind es doch die Cyber-Attacken, welche als besonders große Bedrohung wahrgenommen werden. Eine Umfrage des Bundesamtes für Sicherheit in der Informationstechnik zum Thema „Cyber-Risiken & Schutzmaßnahmen in Unternehmen“ kam zu dem Ergebnis: „**Drei Viertel der Befragten sehen Cyber-Bedrohungen als relevante Gefährdung**“ (vgl. Allianz für Cyber-Sicherheit 2019a, S. 6).

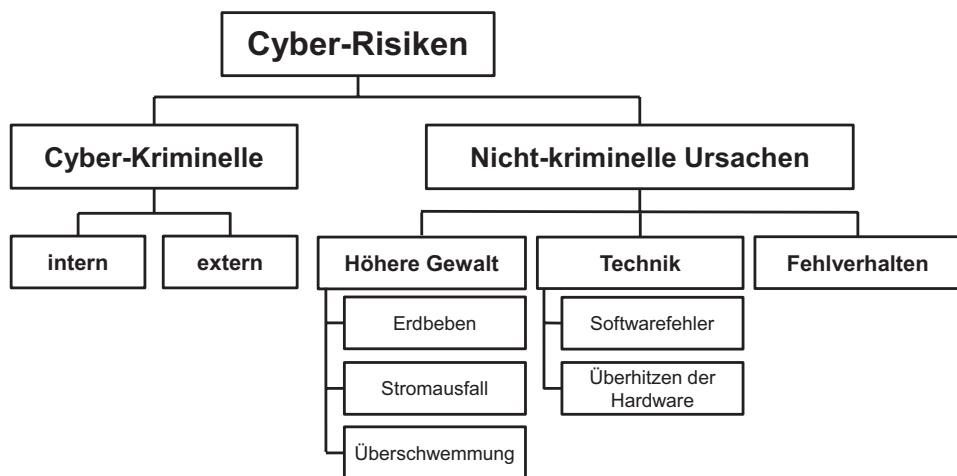


Abb. 21.1 Bedrohungspotenziale. (Quelle: eigene Darstellung in Anlehnung Jung et al. 2016, S. 4)

Die Ziele der Cyber-Kriminellen variieren, so wie die Vorgehensweisen oder die Motivation, die dahintersteckt. Neben der Differenzierung zwischen externen und internen Angreifern sollten bei Cyber-Kriminalität vier verschiedene **Angreifermodelle** unterschieden werden (vgl. Biener et al. 2015, S. 11).

„Eins gegen eins“

Der Angreifer hat sein Ziel aus einem meist persönlichen Grund ausgewählt. Er kennt das Unternehmen und möglicherweise kennt auch das Unternehmen den Angreifer. Als Beispiel wären hier Mitarbeiter bzw. ehemalige Mitarbeiter zu nennen. Die personalisierte Attacke hat meistens Hass, Rache, eine persönliche Bereicherungsabsicht oder Geschäftsspionage bzw. -sabotage als Motiv.

„Eins gegen viele“

Hierbei handelt es sich um eine anonyme Attacke gegen mehrere Ziele. Der Angreifer kennt seine Ziele oft nicht und möchte selbst auch unerkannt bleiben. Bei diesem Angriff steht meistens eine monetäre Bereicherungsabsicht im Vordergrund.

„Viele gegen eins“

Bei dem dritten Modell greifen mehrere Angreifer ein einzelnes Ziel an. Die Angreifer kennen das Ziel, jedoch bleiben die Angreifer für das Ziel anonym. Dieses Angreifer-Modell erfordert einen Zusammenschluss von Cyber-Kriminellen, die hinsichtlich ihres Know-hows in der Lage sind, einen solchen geplanten und koordinierten Angriff durchzuführen. Die Motive dieses Angreifer-Modells können Rache, Hass, Terrorismus oder der Wunsch nach Ruhm sein. Dieses Angreifer-Modell ist typisch für Denial-of-Service-Attacken (vgl. Abschn. 21.2.4.3). Viele dieser Angriffe werden über automatisierte Computerprogramme ausgeführt. Mithilfe sogenannter „Botnetzwerke“ oder „Botnets“ kann ggf. auch ein einzelner Cyber-Krimineller eine solche Attacke ausführen.

„Viele gegen viele“

Hierbei werden viele Ziele von vielen Angreifern attackiert. Wie im „viele gegen eins“-Angreifer-Modell erläutert, findet auch hier ein koordinierter Angriff statt, der eine Organisation der Angreifer voraussetzt. Die sorgfältig ausgewählten Ziele müssen gesammelt werden, bevor der Angriff erfolgen kann. Die Motive dieses Models sind nur selten persönlicher Natur, sondern meist handelt es sich um Hass, Terrorismus oder den Wunsch nach Ruhm (vgl. Biener et al. 2015, S. 12–13).

Ziel einer Cyber-Attacke kann jeder werden! Sowohl Privatpersonen als auch Unternehmen oder sogar ganze Staaten können von einer einzelnen Person oder gut organisierten Hackergruppen ins Visier genommen werden. Große Unternehmen sind für Cyber-Kriminelle besonders attraktiv, da sie durch ihre Finanzkraft eine finanziell lukrative Beute darstellen. Durch die Komplexität großer Unternehmen besteht für die Angreifer außerdem eine geringere Chance entdeckt zu werden (vgl. Flagmeier und Heidemann 2018, S. 29). Entscheidend bei der Art des Angriffes ist die technische Ausstattung und das

Know-how der Angreifer und des Ziels. Einfache Cyber-Kriminelle sind meist Einzelpersonen, die mit geringer Professionalität arbeiten und dementsprechend geringere Schäden verursachen (vgl. Bundesamt für Sicherheit in der Informationstechnik 2019a). Die Bandbreite an Möglichkeiten von organisierten Cyber-Kriminellen hingegen reicht von Identitätsdiebstahl über Warenbetrug bis hin zur Erpressung.

Organisierte Cyber-Kriminelle verfügen über viel Know-how und finanzielle Mittel, weswegen Unternehmen oft das Problem der Konfrontation mit einer **asynchronen Kriegsführung** haben, denn es erfordert meist ebenso viel Expertenwissen und sehr viel mehr finanzielle Mittel, um die Sicherheitsstrukturen eines Unternehmens, eines Staats oder einer Person so aufzurüsten, dass Angriffe ausreichend abgewehrt werden können.

Laut einer Bitkom Studie sind ehemalige Mitarbeiter in 61 Prozent der Fälle für Angriffe auf das Unternehmen verantwortlich. Somit stellen sie hinsichtlich Cyber-Risiken die größte Bedrohung dar. 29 Prozent der Unternehmen wurden in den letzten zwei Jahren von Hobby-Cyber-Kriminellen attackiert. Eine weitere ernst zu nehmende Bedrohung stellen Wettbewerber dar, die in 22 Prozent der Fälle als Angreifer identifiziert werden konnten. 17 Prozent der befragten Unternehmen wurden von professionell organisierten Cyber-Kriminellen attackiert. Besonders große Unternehmen mit mehr als 500 Mitarbeitern wurden aufgrund ihrer wertvollen Daten signifikant häufiger attackiert als kleinere Unternehmen (vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. 2018, S. 28).

21.2.3 Schwachstellen

Bedrohungspotenziale werden erst gefährlich, wenn ein Unternehmen Schwachstellen, wie zum Beispiel Fehler in sicherheitsrelevanten IT-Systemen, Prozessen oder anderen innerbetrieblichen Strukturen, aufweist. Eine Schwachstelle ist ein möglicher Angriffspunkt für Cyber-Kriminelle und ermöglicht es ihnen, sich Zugriff zu den Systemen zu verschaffen. Aber auch nicht-kriminelle Bedrohungspotenziale verursachen an den folgenden Schwachstellen erhebliche Schäden.

Systeme/Hardware

Systeme, Hard- und Software sind die Grundlage der Informationstechnologie und somit der Industrie 4.0. Dadurch sind sie aber auch die offensichtlichste Schwachstelle für Cyber-Kriminalität. Schwachstellen an der Hardware sind zurückzuführen auf das Versagen der physischen Ausstattung, wie zum Beispiel Überalterung, Instandhaltung, Leistungsfähigkeit oder Kapazität. Attraktiver für Cyber-Kriminelle sind aber sicherheitsrelevante Fehler in Software und Systemen, welche Risiken für Unternehmen darstellen. Sicherheitseinstellungen, Programmierpraktiken und Softwareänderungen sind weitere mögliche Schwachstellen.

Aber auch nicht-kriminelle Ursachen können großen Schaden anrichten. So ist es die physisch vorhandene Technik, die bei höherer Gewalt wie Sturm, Brand, Überschwemmung oder Stromausfall, maßgeblich geschädigt wird und somit Datenverluste oder eine

Betriebsunterbrechung zur Folge haben kann. Manchmal kann ein Versagen integrierter Systeme dafür sorgen, dass die Ausführung anders läuft als erwartet (vgl. Biener et al. 2015, S. 6).

Menschen

Die größte Schwachstelle hinsichtlich Cyber-Risiken stellen Menschen bzw. Mitarbeiter dar. Auch hier muss man unterscheiden zwischen dem **vorsätzlichen Handeln** mit der Absicht, Schaden anzurichten, und **unbeabsichtigtem Fehlverhalten**. Die Sensibilisierung der Mitarbeiter für Datensicherheit kann sehr unterschiedlich ausgeprägt sein. Je mehr Mitarbeiter mit sensiblen Daten arbeiten, desto größere Schäden können aus kleinen Fehlern entstehen. Dabei kann es sich natürlich um Irrtümer handeln, wie dem falschen Adressieren einer E-Mail oder dem Verlust von Firmengeräten, wie Smartphones, Notebooks oder Tablets. Auch der Mangel von Fähigkeiten, Fachwissen und der Verfügbarkeit von Personal, kann ein Risiko darstellen (vgl. Biener et al. 2015, S. 10).

Insbesondere in Bezug auf Cyber-Kriminalität werden Mitarbeiter oftmals zum Ziel, um sich Zugang zu Gebäuden, Systemen oder sensiblen Daten zu verschaffen. Cyber-Attacken im Rahmen des sogenannten Social Engineerings (vgl. Abschn. 21.2.4.2) nutzen gezielt Menschen für ihre kriminellen Taten. Unzureichende Schulungen und unvorsichtiges Verhalten stellen hier ein großes Problem dar und machen diese Cyber-Attacken oft erst möglich.

Mitarbeiter können somit Opfer einer Cyber-Attacke werden. Häufig sind es aber auch genau diese, welche vertrauliche Informationen stehlen und somit das Unternehmen bewusst schädigen. Besonders ehemalige Mitarbeiter stellen mit 61 Prozent den Großteil der Angreifer dar (vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. 2018, S. 28). Die Gelegenheit dazu ergibt sich bereits während der aktiven Tätigkeit im Unternehmen. In dieser Zeit kann ein Mitarbeiter, der kriminelle Absichten verfolgt, Informationen sammeln, sich Zugriffe verschaffen und die Prozesse des Unternehmens auf mögliche Angriffspunkte untersuchen.

Prozesse

Der Zugriff zu sensiblen Unternehmensdaten muss strikt geregelt sein. Das „Need to know“-Prinzip besagt, dass Mitarbeiter nur Zugang zu Informationen erhalten sollten, die für die Erfüllung ihrer Aufgaben erforderlich sind. Allerdings funktioniert das Beschränken der Zugänge besonders in kleinen und mittelständischen Unternehmen nur unzureichend, denn dort haben oft selbst Praktikanten uneingeschränkten Zugang (vgl. Heisz et al. 2017, S. 8). Nicht nur Zugriffsrechte auf Informationen spielen eine Rolle, sondern auch der Zugang zu Gebäuden sollte nur restriktiv gewährt werden (vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. 2018, S. 40). Unzureichende Kontrollen, unklare Regelungen bezüglich Sicherheitsvorkehrungen, nicht vorhandene Zertifizierungen und nicht klar definierte Zuständigkeiten führen oft zu nicht trivialen Sicherheitslücken (vgl. Biener et al. 2015, S. 8).

21.2.4 Cyber-Attacken

21.2.4.1 Malware

Malware ist der häufigste Fall von Cyber-Kriminalität und spielt in 30 Prozent aller Cyber-Attacken weltweit eine Rolle (vgl. Marinos und Lourenço 2019, S. 26). Der Begriff Malware wird abgeleitet von dem Begriff „Malicious Software“ und wird häufig auch als Schadfunktion, Schadprogramm und Schadsoftware bezeichnet. Malware ist somit eine Software, die entwickelt wurde, um gezielt Schäden in Systemen anzurichten. Beispiele für Malware sind Viren, Würmer, Spyware, Trojaner, Keylogger und Ransomware (vgl. Bundesamt für Sicherheit in der Informationstechnik 2019b). Dabei werden Schwachstellen in IT-Systemen des Unternehmens genutzt, um Informationen zu manipulieren, zu löschen oder zu stehlen. Die Malware befindet sich oft als Anhang an einer Spam-Mail oder auf bösartigen Webseiten und wird durch Anklicken heruntergeladen und automatisch auf dem Gerät installiert. Der Anteil der E-Mails, die als Spam kategorisiert werden, stieg die letzten Jahre kontinuierlich an. Im Jahr 2018 wurden mit 55 Prozent mehr als die Hälfte der eingehenden E-Mails als Spam eingestuft (vgl. Marinos und Lourenço 2019, S. 23). Damit sich Unternehmen gegen Malware-Attacken schützen können, bedarf es technischer Sicherheitsvorkehrungen, wie zum Beispiel durch Spam-Filter.

„WannaCry“

Besonders viel Aufmerksamkeit erregte die Malware „WannaCry“ Mitte Mai 2017. Dabei handelte es sich um eine Ransomware (auch „Krypto Trojaner“ genannt), die speziell für Windows-Betriebssysteme entwickelt wurde und 2017 mindestens 220.000 Windows-Rechner infizierte. Möglich war dies durch eine Sicherheitslücke, welche als „Eternal Blue“ bekannt ist. WannaCry chiffrierte die Daten der Computer und hinterließ eine Nachricht, welche die Unternehmen dazu aufforderte, innerhalb von sieben Tagen eine Lösegeldzahlung in Höhe von 300 US-Dollar zu leisten, da ansonsten alle Daten gelöscht würden. Die 300 US-Dollar sollten in Form von Bitcoins auf eins von fünf Konten überwiesen werden. Die Kryptowährung Bitcoin ist bei Cyber-Kriminellen besonders beliebt, da Transaktionen damit zwar beobachtet werden können, der Inhaber des Bitcoin-Kontos aber anonym bleibt (vgl. Reynolds 2017). Im Falle von WannaCry hat Microsoft zwar sehr zügig ein Sicherheitsupdate veröffentlicht, jedoch gibt es auch heute noch Opfer, die Lösegeldzahlungen auf die WannaCry-Bitcoin-Konten leisten (Actual ransom 2019). Typisch für Malwareschäden ist (wie im Fall von WannaCry) die Höhe des Schadens. Malware verursacht meist hohe kumulative Schäden anstatt hoher Einzelschäden (vgl. Biener et al. 2015, S. 22). ◀

21.2.4.2 Social Engineering

Social Engineering ist eine Form von Cyber-Attacke, bei denen Kriminelle menschliche Schwachstellen wie Neugier, Angst oder Unwissenheit ausnutzen, um ihre Ziele zu erreichen. Dabei werden Menschen gezielt manipuliert, um daraufhin freiwillig sensible Daten

preiszugeben, die den Kriminellen dabei helfen, Schutzmaßnahmen zu umgehen oder Malware (vgl. Abschn. 21.2.4.1) auf die Systeme der Betroffenen zu installieren (vgl. Bundesamt für Sicherheit in der Informationstechnik 2019b). Die Arten des Social Engineerings sind sehr vielfältig und erfolgen sowohl per E-Mail, per Telefon, aber auch persönlich. Laut Bitkom-Studie gab es bei 13 Prozent der befragten Unternehmen Fälle von analogem Social Engineering, elf Prozent gaben an, Opfer von digitalem Social Engineering geworden zu sein (vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. 2018, S. 15). Um sich Zugriff zu sensiblen Daten oder Gebäuden zu verschaffen, nutzen Cyber-Kriminelle die Hilfsbereitschaft, Gutgläubigkeit oder Unsicherheit des Opfers aus (vgl. Biener et al. 2015, S. 14).

Nachfolgend sind zwei Beispiele von Social Engineering aufgeführt, wobei Phishing zwar besonders häufig vorkommt, die Vorgehensweise beim „Fake President Fraud“ für Cyber-Kriminelle jedoch lukrativer ist.

Phishing

Eine besonders häufige Form des Social Engineering ist das sogenannte „Phishing“, welches sich aus dem Wort „Password“ und „Fishing“ zusammensetzt und auf Deutsch „nach Passwörtern angeln“ bedeutet. Hierbei wird das Opfer mittels gefälschter E-Mails und/oder Webseiten dazu aufgefordert, Zugangsdaten preiszugeben. Besonders häufig werden Bankkunden in angeblichen E-Mails ihrer Bank dazu aufgefordert, Kontodaten einzugeben, welche von Cyber-Kriminellen später genutzt werden, um Geld von den Konten zu entwenden (vgl. Bundesamt für Sicherheit in der Informati-onstechnik 2019b).

Phishing-E-Mails sind heutzutage sehr gut gefälscht, so dass es den Opfern schwerfällt, den Betrug zu erkennen. Moderne Spam-Filter erkennen Phishing-Attacken allerdings immer zuverlässiger, was dazu führt, dass, obwohl 55 Prozent aller E-Mails im Jahr 2018 als Spam eingestuft wurden, der Anteil der Phishing E-Mails innerhalb der letzten fünf Jahre kontinuierlich sinkt (2017 war eine von 2995 E-Mails eine Phishing-Attacke, 2018 sank die Rate auf eine von 3207 (vgl. Symantec 2019, S. 23)). ◀

„Fake President Fraud“

Eine für Cyber-Kriminelle sehr lukrative Form des Social Engineerings ist der sogenannte „Fake President Fraud“. Cyber-Kriminelle geben sich dabei als Vorstands- oder Mitglied der Geschäftsführung aus und bitten per E-Mail, Fax oder Telefon solche Mitarbeiter, die im Unternehmen für Banktransaktionen verantwortlich sind, eine dringende Überweisung auszuführen. Die Täter gehen dabei hochprofessionell vor: Vor der Aktion werden monatlang die zuständigen Mitarbeiter des Unternehmens ausspioniert, sodass die Aktion absolut überzeugend durchgeführt werden kann. Die Vorgehensweise ist meist für den Mitarbeiter nicht als Betrug erkennbar, da die Täter gefälschte E-Mails und sogar gestohlene Unterschriften nutzen, um die notwendige Glaubwürdigkeit zu erzeugen. Dem Mitarbeiter wird dabei suggeriert, es handele sich um eine höchst geheime und besonders vertrauliche Angelegenheit, die weitreichende Auswirkungen für den Erfolg des

Unternehmens hat. Geschmeichelt von dem Vertrauen, welches die Geschäftsleitung dem Mitarbeiter entgegenbringt, sind sie oft bereit, die Transaktion dann auszuführen. Dabei wird Druck ausgeübt, damit die Transaktion möglichst zügig ausgeübt wird. Bemerkt der Mitarbeiter den Schwindel nicht rechtzeitig, ist das Geld bereits auf ausländischen Konten. Dadurch wird es schwer, das Geld zurückzuholen. Außerdem erschwert häufig das ausländische Rechtssystem die schnelle Behebung des Schadens.

Weltweit erbeuten Cyber-Kriminelle durch diese Betrugsmasche Millionen von den betroffenen Unternehmen. Der „Fake President Fraud“ baut darauf auf, dass die Opfer vom angeblichen Geschäftsführer suggeriert bekommen, es handelt sich um eine besonders vertrauliche Angelegenheit. Darauf wird im Schriftverkehr, der ausschließlich per E-Mail erfolgen soll, mehrfach hingewiesen. Ein weiterer Täter nimmt die Rolle eines Anwalts in einer Kanzlei ein, welcher über Telefon die Transaktion in die Wege leiten soll. Die Kontaktdaten werden gleich mitgeliefert und auch hierbei weist der vermeintliche Anwalt auf die hohe Geheimhaltungsstufe hin. Der Mitarbeiter wird angewiesen, nur über diese zwei Kommunikationswege zu agieren. Hält der Mitarbeiter sich an die Vorgaben und spricht mit niemandem über die Transaktion, ist der „Fake President Fraud“ erfolgreich (vgl. Flagmeier und Heidemann 2018, S. 26–28). ◀

21.2.4.3 Distributed Denial of Service (DDoS)

Bei einem „Denial of Service (DoS)“-Angriff wird der Zugriff auf ein System gestört oder selbiges sogar zum Erliegen gebracht. Handelt es sich bei dem Ziel um ein Netzwerk von Systemen, spricht man von einem „Distributed Denial of Service (DDos)“-Angriff (vgl. Biener et al. 2015, S. 14). Bei DDoS-Angriffen werden die Systeme überlastet, damit sie den Nutzern nicht mehr zur Verfügung stehen. Dies geschieht durch den gemeinsamen Angriff von organisierten Cyber-Kriminellen oder durch einen Einzelnen, der mithilfe eines Bot-Netzwerkes die nötige Angriffsstärke erzielt (vgl. Biener et al. 2015, S. 13). Verschiedene technische Schwachstellen ermöglichen DDoS Angriffe, wie zum Beispiel das Überlasten des Arbeitsspeichers und der Prozessoren, wenn diese nicht auf solche Mengen an Datenverkehr ausgerichtet sind. Volumenbasierte Angriffe, zum Beispiel in Form eingehender Datenpakete, können einen Router in seiner Funktion beeinträchtigen und ihn schlussendlich funktionsunfähig machen, da er für Anfragen nicht mehr erreichbar ist.

Die Nichterreichbarkeit kann zu finanziellen Schäden, zum Beispiel zu Umsatzeinbußen sowie Reputationsschäden, führen. Cyber-Kriminelle nutzen DDoS-Angriffe, um Unternehmen, vor allem Unternehmen im Online-Handel oder Onlinebanking-Portale, zu erpressen. Dabei ist ähnlich wie bei Ransomware von einer Zahlung des geforderten Lösegelds abzusehen, da dies die Kriminellen nur in ihrem Tun unterstützt (vgl. Pohlmann und Fritzen 2015, S. 60).

DDoS-Angriffe sind für Kriminelle ein lukratives Geschäftsmodell, denn sie richten nicht nur viel Schaden an, sondern sind auch erschreckend einfach in Gang zu setzen. Es existieren zum Beispiel spezielle Webseiten, auf denen DDoS-Angriffe als Dienstleistung in Auftrag gegeben werden können (*asynchrone Kriegsführung*; vgl. Akamai 2018, S. 24). Laut „Internet Security Threat Report“ kostet ein kleiner DDoS-Angriff, der weniger als

eine Stunde dauern soll, circa fünf bis 20 US-Dollar, ein Angriff über mehr als 24 Stunden hingegen kann zwischen zehn und 1000 US-Dollar kosten (vgl. Symantec 2019, S. 58). Ein kleiner Preis für den möglichen Schaden, der dadurch angerichtet werden kann. Es ist also nicht verwunderlich, dass die Anzahl der DDoS-Angriffe von 2017 auf 2018 um 16 Prozent angestiegen ist (vgl. Akamai 2018, S. 2).

21.3 Risikomanagement

Um sich vor Cyber-Attacken ausreichend schützen zu können, müssen Unternehmen ein umfassendes Risikomanagement implementieren. „Unter Risikomanagement wird die Messung und Steuerung aller betriebswirtschaftlichen Risiken unternehmensweit verstanden“ (vgl. Wolke 2009, S. 1). Das Risikomanagement beschäftigt sich folglich mit der Identifizierung, Analyse und Bewertung von sämtlichen für das Unternehmen relevanten Risiken. Dabei unterstützt das Risikomanagement die Entscheidungsfindung bzgl. übergeordneter Ziele, Strategien und Politik des Unternehmens. Die gesamtunternehmerische Risikobeurteilung soll der Planungssicherheit dienen und die interne und teils externe Berichterstattung soll für Transparenz sorgen. Die identifizierten Risiken werden nach bestimmten Kriterien beurteilt und es werden dementsprechende Maßnahmen zur Risikovermeidung oder -reduzierung eingeleitet.

Das Risikomanagement soll laut der Norm ISO 31000 als Aufgabe des Managements verstanden werden, da es sich um einen fortlaufenden Prozess handelt, welcher alle Bereiche des Unternehmens betrifft. Die Norm legt zusätzlich Leitlinien zum Umgang mit Risiken innerhalb eines Unternehmens fest. Der Standard ist ein allgemeiner Ansatz, welcher nicht branchenspezifisch ist und sich somit auch auf Risiken aller Art anwenden lässt. Dieser fortlaufende Risikomanagementprozess ist in ◉ Abb. 21.2 dargestellt.

Zu Beginn dieses Prozesses steht die **Risikoidentifizierung** (vgl. Abschn. 21.3.2) und somit die Beschreibung der Risiken, ihrer Ursachen und Auswirkungen. Die **Analyse** (vgl. Abschn. 21.3.2) beschäftigt sich mit den aus dem Risiko resultierenden möglichen Schäden und ihren Eintrittswahrscheinlichkeiten. Die **Risikobewertung** (vgl. Abschn. 21.3.2) bedarf dem vorherigen Festlegen von Kriterien. Anschließend werden im Rahmen der Risikobehandlung geeignete **Maßnahmen** (vgl. Abschn. 21.3.3) ergriffen, um die im Prozess identifizierten Risiken zu minimieren. Es handelt sich dabei um einen iterativen Prozess, welcher kontinuierliche Überwachung und Kontrolle erfordert.

21.3.1 Stakeholder

Durch einen proaktiven Umgang mit Risiken können Unternehmen auf das Schadenausmaß und die Eintrittswahrscheinlichkeit einwirken und somit die finanzielle Belastung senken, welches im Interesse aller Stakeholder ist. Stakeholder sind „alle internen und externen Personengruppen, die von den unternehmerischen Tätigkeiten gegenwärtig oder

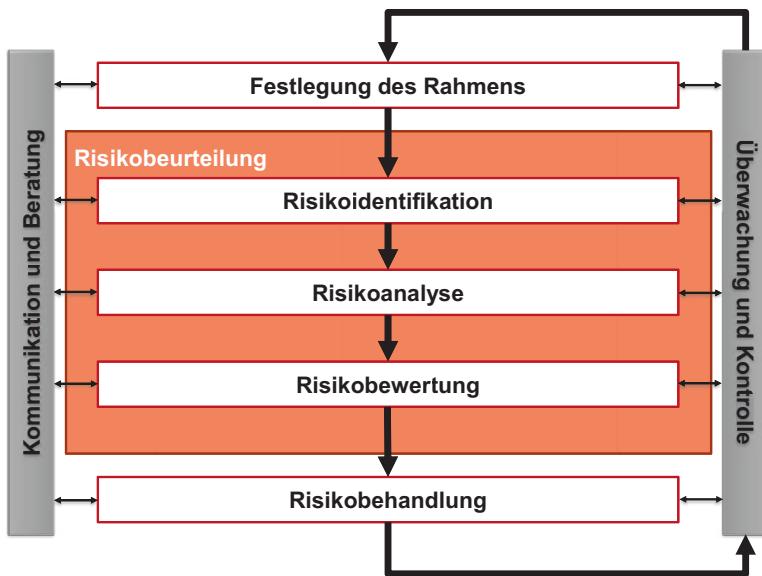


Abb. 21.2 Risikomanagementprozess. (Quelle: eigene Darstellung in Anlehnung DIN ISO 31000)

in Zukunft direkt oder indirekt betroffen sind“ (vgl. Thommen 2019). Um ein Unternehmen erfolgreich zu führen, müssen alle Stakeholdergruppen bei Entscheidungen, die dem Unternehmenserfolg dienen sollen, berücksichtigt werden. Die internen und externen Stakeholder, die Interesse an der Implementierung eines funktionierenden Risikomanagements zur Abwehr von Cyber-Risiken haben, besitzen unterschiedliche Erwartungen an das Unternehmen und sind teils mehr, teils weniger in das Risikomanagement involviert.

Sobald ein Cyber-Angriff erfolgreich ist, kann daraus auch ein monetärer Schaden für die Eigentümer des Unternehmens resultieren. Der Vorstand ist laut § 91 Abs. 2 AktG dazu verpflichtet, ein Risikofrüherkennungs- und Überwachungssystem im Unternehmen zu implementieren. Das Risikomanagement ist also als Aufgabe des Managements zu verstehen und nur zusammen mit einer funktionierenden Risikokultur unter den Mitarbeitern lassen sich gesamtunternehmerische Ziele verfolgen. Aus Sicht der Mitarbeiter ist die Insolvenzabsicherung des Unternehmens nicht zuletzt aufgrund der Sicherung des eigenen Lebensunterhaltes von entscheidender Bedeutung. Neben diesen sogenannten internen Stakeholdern kann es noch eine Reihe externer Stakeholder, wie zum Beispiel Fremdkapitalgeber, Staat und Gesellschaft, geben. Hinsichtlich der durch die Digitalisierung verbundenen Wertschöpfungskette verschiedenster Unternehmen, ist es für Lieferanten und Kunden von besonderer Bedeutung, dass ein Unternehmen in der Lage ist, Risiken frühzeitig zu erkennen, zu verringern oder gar zu vermeiden. Aufgrund der digitalen Verknüpfung kann ein Cyber-Risiko besonders bei Lieferanten und Kunden auf deren Systeme übertragen werden und Schaden anrichten (vgl. Thommen 2019).

Die unterschiedlichen Erwartungen einzelner Stakeholder-Gruppen machen die Einrichtung eines gesamtunternehmerisch ausgerichteten Risikomanagements für Cyber-Risiken notwendig, damit die Unternehmen etwaige Cyber-Risiken bewältigen können (vgl. Wrede et al. 2019 S. 420).

21.3.2 Risikoidentifizierung, -analyse und -bewertung

Der Risikomanagementprozess nach ISO 31000 umfasst die Risikoidentifizierung, -analyse und -bewertung. Um geeignete Maßnahmen gegen Cyber-Risiken einleiten zu können, bedarf es einer umfassenden Analyse. Diese wird auch „Cyberrisk-Assessment“ genannt. Die Schwachstellen im Unternehmen können zum Beispiel organisatorischer, technischer oder personeller Natur sein. Meist ist es eine Kombination mehrerer Schwachstellen, welche den Angreifern Zugang zum Unternehmen verschafft. Zum Beispiel wird Social Engineering (vgl. Abschn. 21.2.4.2) oft genutzt, um Malware (vgl. Abschn. 21.2.4.1) in den Systemen zu platzieren.

Für die **Risikoidentifizierung** müssen sich Unternehmen fragen, welche Vermögenswerte im Unternehmen von Risiken bedroht werden bzw. welche Stellen anfällig für potenzielle Schäden sind. Sind sie für Schäden an Dritten haftbar? Sind ihre Mitarbeiter ausreichend geschult und vertrauenswürdig? Das Auffinden interner nicht-krimineller Cyber-Risiken ist meist einfacher, als die möglichen Angriffspunkte von Cyber-Kriminellen zu finden, da keine menschliche Motivation und keine Taktik dahinterstecken. Diese Fragestellungen müssen im Prozess der Risikoidentifizierung beantwortet werden, und zwar systematisch und vor allem kontinuierlich. Dazu werden verschiedene Methoden genutzt, zum Beispiel Betriebsbesichtigungen, Befragungen, Szenario-Analysen, Simulationen oder auch der Einsatz von Schwachstellen-Scanning-Programmen (vgl. Königs 2017, S. 418).

Die **Risikoanalyse** beschäftigt sich mit der Eintrittswahrscheinlichkeit des potenziellen Schadenereignisses. Um die Schadenereignisse angemessen einstufen zu können, bedarf es vielfältiger Methoden, wie zum Beispiel die Durchführung von Befragungen und Ursachenanalysen. Darüber hinaus muss die Interdependenz zwischen den verschiedenen Risiken berücksichtigt werden. Da die Vorgehensweise der Cyber-Kriminellen zunehmend professioneller wird, müssen auch die Methoden der Risikoanalyse kontinuierlich weiterentwickelt werden.

Besonders die **Risikobewertung** ist für spätere Maßnahmen essenziell, da besonders die Relevanz bzw. die potenzielle Schadenhöhe darüber entscheidet, welche Maßnahme gewählt werden soll. Schwachstellen, die von Cyber-Kriminellen genutzt werden, sind besonders schwer zu bewerten, da die Motivation, Taktik und Angriffsmethode des Cyber-Kriminellen, aber auch die Ernsthaftigkeit in Bezug auf einen Schaden, eine wichtige Rolle spielt (vgl. Königs 2017, S. 419).

21.3.3 Maßnahmen

Als Maßnahmen werden im Risikomanagement alle Aktionen bezeichnet, die dazu dienen, Risiken zu vermeiden, zu reduzieren oder zu transferieren. Unternehmen können organisatorische, personelle, technische sowie prozessbezogene Maßnahmen einleiten, um die Risiken zu kontrollieren (vgl. Bundesamt für Sicherheit in der Informationstechnik 2019a). Solche Maßnahmen können zwar nie einen 100-prozentigen Schutz bieten, jedoch stellen sie mit Blick auf eine eventuell zu implementierende Versicherungslösung (vgl. Abschn. 21.4) die Versicherungsfähigkeit her bzw. führen ggf. zu einer für das Unternehmen günstigeren Prämie. Risikopolitische Maßnahmen stoßen oft auf Widerstand, da Risiken von Stakeholdern subjektiv wahrgenommen werden. Somit ist es wichtig, die Sinnhaftigkeit der Maßnahmen zu kommunizieren und eine Risikokultur im Unternehmen zu etablieren.

21.3.3.1 Risikovermeidung

Die Maßnahmen zur Risikovermeidung, welche Risiken mittels der Verringerung der Eintrittswahrscheinlichkeit vorbeugen, lassen sich in drei Kategorien unterteilen: IT-Sicherheitsstandards, Kompetenz der Belegschaft und organisatorische Sicherheitsvorkehrungen. Nur die Kombination der verschiedenen Maßnahmen kann einen gesamtunternehmerischen Schutz vor Cyber-Risiken bieten.

IT-Sicherheitsstandards

Die meisten Unternehmen verfügen über einen technischen Basisschutz, wie zum Beispiel Passwortschutz, VirensScanner und Firewalls auf allen technischen Geräten. Regelmäßige Backups zur Datensicherung werden inzwischen automatisch durchgeführt. Dieser Basis schutz reicht jedoch selten aus, um Cyber-Kriminelle von einem Angriff abzuhalten, denn diese haben das Know-how, um gängige Sicherheitsvorkehrungen zu umgehen und entwickeln mit der Zeit immer mehr Taktiken, um auch neuste Sicherheitsmaßnahmen zu überwinden. Deswegen müssen Unternehmen kontinuierlich an ihren IT-Sicherheitsstandards arbeiten, um dieser Entwicklung entgegenzuwirken (vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. 2018, S. 56).

Kompetenz der Belegschaft

Ungenügendes Risikobewusstsein und unachtsames Verhalten der Mitarbeiter ist der Grund, warum Social Engineering (vgl. Abschn. 21.2.4.2) so erfolgreich ist. Die Sensibilisierung für Cyber-Risiken kann durch spezifische Schulungen, wie zum Beispiel zu den Themen Spionage, Sabotage und Datendiebstahl, erfolgen. Mitarbeiter müssen Cyber-Risiken als Bedrohung wahrnehmen und die Sinnhaftigkeit der Sicherheitsvorkehrungen verinnerlichen, um im Ernstfall Gefahren zu erkennen und richtig zu handeln. Zur personellen Sicherheit gehören Background-Checks von Mitarbeitern, die sensible Positionen belegen. Außerdem sollten Mitarbeiter die Chance haben, mittels eines Whistle-Blowing-Tools anonym auf verdächtiges Mitarbeiterverhalten hinweisen zu können (vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. 2018, S. 56).

Organisatorische Sicherheitsvorkehrungen

Zu den prozessbezogenen Maßnahmen gehören die Beschränkung von Zugriffsrechten auf sensible Daten sowie die Kontrolle der physischen Zugangsrechten zu bestimmten Bereichen. Betriebsgeheimnisse und andere sensible Daten sollten dementsprechend gekennzeichnet werden und es muss klare Regeln für den Umgang mit schützenswerten Informationen geben. Weitere Maßnahmen sind eine „Clean-Desk-Policy“, regelmäßige Sicherheitsaudits und eine adäquate Zertifizierung (vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. 2018, S. 40). Unternehmen sind sich oft nicht bewusst, ob und wann sie für Schäden durch Dritte haftbar gemacht werden können. Daher ist es sinnvoll, dieses Thema in der Organisation zu betrachten und entsprechende Vorkehrungen zu treffen.

21.3.3.2 Risikoreduzierung

Maßnahmen zur Risikoreduzierung setzen an der Verminderung der Schadenhöhe an, das heißt, sobald ein Schaden eintritt, sind Maßnahmen zu ergreifen. Dazu sollten Unternehmen ein professionelles Notfallmanagement etablieren. Teilweise bieten Versicherungen im Rahmen einer Cyber-Versicherung verschiedene Serviceleistungen an, die dem Kunden helfen, richtig zu reagieren (vgl. Abschn. 21.4.3) (vgl. Heisz et al. 2017, S. 8). Im Krisenfall kommt es auf eine schnelle Reaktion und klare Zuständigkeiten an (vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. 2018, S. 56). Es bedarf schriftlich geregelter Abläufe und einer schnellen Analyse des Vorfallses, um dem Schaden entgegen wirken zu können. Aufmerksame und geschulte Mitarbeiter können hier erheblich zur Reduktion des Schadens beitragen (vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. 2018, S. 30).

21.3.3.3 Risikotransfer

Der Risikotransfer (auch Risikoüberwälzung genannt) ist eine Variante der Risikohandhabung. Im Gegensatz zur Risikovermeidung und -reduzierung werden beim Risikotransfer weder Eintrittswahrscheinlichkeit noch Schadenausmaß reduziert. Stattdessen werden die aus dem Risiko resultierenden Konsequenzen vom ursprünglichen Risikoträger an einen oder mehrere Dritte übertragen, im Regelfall über eine Versicherung. Es muss zwischen einer vollständigen und einer anteiligen Versicherung der abzusichernden Risiken unterschieden werden. Der Risikotransfer erfolgt mittels eines Versicherungsunternehmens, welches im Rahmen der Versicherungslösung die Risiken des Unternehmens übernimmt und als Gegenleistung hierfür eine Prämie verlangt.

Im Risikomanagement von Unternehmen fehlt oft die interdisziplinäre Fachexpertise, die es benötigt, um Cyber-Risiken in ihrem vollen Umfang zielgerichtet erfassen und bewältigen zu können. Das Erfordernis zur Absicherung gegen Cyber-Risiken wird somit durch eine entsprechende Versicherungslösung abgedeckt, welche im folgenden Abschnitt ausführlich beschrieben wird (vgl. Abschn. 21.4). Trotz Versicherungslösung verbleiben dem Unternehmen aber Restrisiken, zum Beispiel durch Selbstbehalte, eine im Schadenfall unzureichende Versicherungssumme oder durch das Ausfallrisiko bei einer möglichen Insolvenz des Vertragspartners.

21.3.3.4 Risikoakzeptanz

Auch wenn die Möglichkeiten für die Risikobewältigung vielfältig sind, sollten Unternehmen abwägen, ob die Maßnahmen zur Risikovermeidung, -reduzierung oder -transfer wirtschaftlich vertretbar sind. Übersteigen die Kosten für solche Maßnahmen die potenzielle Schadenhöhe, so kann es sinnvoller sein, das Risiko in Kauf zu nehmen. Gelten die Risiken als vertretbar, spricht man von der sogenannten Risikoakzeptanz. Da es sich bei Cyberangriffen um neuartige, sich kontinuierlich wandelnde Risiken handelt, zu denen es bisher keine gesicherten Schadenerfahrungen gibt, sind derartige Risiken für Unternehmen und Versicherer noch schwer zu kalkulieren.

21.4 Versicherungslösungen

Mit der zunehmenden Bedeutung von Cyber-Risiken steigt auch das Angebot an Cyber-Versicherungen, welche als Industriever sicherung Unternehmen die Möglichkeit des Risikotransfers bieten. Wer sich für den Risikotransfer mittels einer Versicherungslösung entscheidet, muss sich seiner Risiken bewusst werden und sich analytisch mit ihnen auseinandersetzen, um dann definieren zu können, welche Absicherung inhaltlich und der Höhe nach überhaupt benötigt wird. Falls dann eine Cyber-Versicherung in Erwägung gezogen wird, sollte zunächst eine Bestandsaufnahme der bisherigen Versicherungsverträge stattfinden, damit das potenzielle Deckungsangebot sich nicht mit den bisherigen Versicherungen überschneidet (vgl. Flagmeier und Heidemann 2018, S. 43).

21.4.1 Silent Cyber

Infolge des digitalen Fortschritts verändern sich auch die Cyber-Risiken stetig. Weder Kunden noch die Versicherungswirtschaft können den Umfang von Cyber-Risiken aktuell ausreichend erfassen bzw. einschätzen. Dies führt dazu, dass traditionelle Industriever sicherungsverträge nur bedingt Cyber-Bausteine enthalten bzw. Cyber-Risiken nicht notwendigerweise explizit ein- oder ausgeschlossen werden. Diese unbekannte Exponierung in den unterschiedlichen Sparten wird als „Silent Cyber“ bezeichnet. Schäden in diesem Bereich sind oft spartenübergreifend und es ist für Versicherungsunternehmen eine Herausforderung abzuschätzen, welche Risiken betroffen sind (vgl. Marsh 2019, S. 13). Wenn Cyber-Kriminelle zum Beispiel Transportsysteme attackieren, um einen Zug entgleisen zu lassen, entstehen hohe Sach- und Personenschäden, die verschiedene Versicherungssparten betreffen. Die größten Herausforderungen für Versicherer sind somit nicht nur Änderungs- und Kumulrisiken, sondern die „unentdeckte Exponierung“. Gemeinsam arbeitet die Versicherungswirtschaft an einer ganzheitlichen Risikoanalyse, um die Einzelkomponenten des „Silent Cyber“-Risikos zu definieren und mehr Transparenz zu schaffen (vgl. Marsh 2019, S. 13).

Die Gefahr besteht, dass Versicherungsunternehmen ihre dadurch entstehenden Probleme an die versicherungnehmende Wirtschaft übertragen, indem sie durch Re-Underwriting und Ausschlüsse Cyber-Risiken aus bestehenden Deckungen herausnehmen, ohne dies in der Preisfindung für diese zu berücksichtigen. Separate Cyber-Deckungen, welche nur durch zusätzliche Prämien erworben werden können, müssen dann von der versicherungnehmenden Industrie zusätzlich finanziert werden. Daher müssen Industrie und Versicherungswirtschaft zusammenarbeiten, um eine Lösung zu finden, welche beiden Parteien gerecht wird (vgl. Siebert 2019).

21.4.2 Klassische Versicherungen

Auf dem Versicherungsmarkt finden sich seit Jahren klassische Versicherungsprodukte, die sowohl die für die Datenverarbeitung erforderlichen Hardware als auch die zugehörige Software innerhalb ihres Deckungsumfangs absichern. Diese Absicherungen für die IT-Nutzung bieten zwar einen Basisschutz, jedoch sollten Unternehmen sich hinsichtlich einer adäquaten Absicherung mit den Bedingungswerken der klassischen Versicherungen auseinandersetzen.

Die **Sach- und Ertragsausfall-Versicherung** bietet Versicherungsschutz für Schäden an versicherten Sachen als Folge einer versicherten Gefahr und für fortlaufende Kosten und entgangene Gewinne infolge dieses Schadenereignisses. Beispielhaft hierfür wäre zum Beispiel ein Brand infolge eines Cyber-Vorfalls, vorausgesetzt der Sachschaden ist laut der Versicherungsfalldefinition abgedeckt. Nach den Grundsätzen der Sach- und Ertragsausfall-Versicherung sind diese Schäden grundsätzlich gedeckt, sofern kein Ausschlussstatbestand besteht.

Die **Betriebshaftpflichtversicherung** inkl. IT-Nutzerdeckung spielt insbesondere für die Absicherung von Schäden bei Dritten und die hieraus folgende Haftung für das Unternehmen eine wichtige Rolle. Sie deckt die gesetzliche Haftpflicht aufgrund Schäden von Dritten aus dem Austausch, der Übermittlung und der Bereitstellung elektronischer Daten. Die IT-Nutzerdeckung ist insbesondere hinsichtlich der geltenden Datenschutzgesetze ein wichtiger Bestandteil einer Absicherung durch Versicherung, da besonders Datenschutzverstöße nicht nur ein monetäres Risiko, sondern auch ein Reputationsrisiko darstellen können. Ein fremder Ertragsausfallsschaden fällt allerdings nicht unter den Deckungsumfang und zusätzlich können weitere Ausschlusstatbestände bestehen, die vom Unternehmen beachtet werden müssen.

Die **Vertrauensschadenversicherung** bietet Schutz für Schäden, die einem versicherten Unternehmen von einer Vertrauensperson oder einem Dritten durch vorsätzliche unerlaubte Handlungen unmittelbar zugefügt werden, vorausgesetzt, sie verpflichten nach gesetzlichen Bestimmungen zum Schadenersatz. Dabei müssen Unternehmen nicht nur den Grund und die Höhe des Schadens definieren können, sondern sie müssen auch die Unmittelbarkeit beweisen können. Mittelbare Verluste sind nicht abgedeckt, wie zum Beispiel entstehende Kosten zur Wiederherstellung der Unternehmensreputation nach einem Da-

tenverlust. Besonders hinsichtlich des von Social Engineering (vgl. Abschn. 21.2.4.2) ausgehenden Cyber-Risikos ist die Vertrauensschadenversicherung eine sinnvolle Absicherung, da Cyber-Policen Fälle, wie zum Beispiel kriminelle Identitätstäuschung, nicht abdecken (vgl. Tittko 2018, S. 29 f.).

21.4.3 Cyber-Policen

Cyber-Policen werden immer beliebter, sodass 14 Prozent der Unternehmen bereits eine solche Versicherung abgeschlossen haben (vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. 2018, S. 51). Schon Mitte der 2000er-Jahre haben sich Cyber-Policen als eigenständiges Produkt am Markt entwickelt, um Unternehmen umfassenden Schutz vor Cyber-Risiken zu bieten. Allerdings hat sich Cyber-Versicherung, zumindest in Deutschland, erst in den letzten fünf bis zehn Jahren erfolgreich als eigenständige Versicherungssparte entwickelt. Die Produktlösungen am Markt zeichnen sich durch eine hohe Komplexität aus (vgl. Wrede et al. 2019, S. 407). Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) hat unverbindliche Musterbedingungen für Cyber-Versicherungen (vgl. Tab. 21.1) veröffentlicht, um insbesondere kleinen und mittelständigen Unternehmen den Risikotransfer zu erleichtern. Die grundlegenden Komponenten sind meistens gleich, doch je größer das Unternehmen, desto komplexer ist der Prozess der Angebotserstellung. Große Unternehmen kommen nicht um eine umfassende Unternehmensanalyse herum, jedoch sind diese es ohnehin gewohnt, individuelle Angebote zu vereinbaren. Bei kleinen und mittelständischen Unternehmen wird aufgrund des Prämienvolumens keine kostenintensive Risikoanalyse durchgeführt, sondern es werden Fragebögen genutzt, um den Bedarf und das Risiko einzuschätzen zu können (vgl. Flagmeier und Heidemann 2018, S. 49).

Tab. 21.1 Musterbedingungen des GDV für eine Cyber-Police. (Quelle: eigene Darstellung in Anlehnung an Gesamtverband der Deutschen Versicherungswirtschaft 2018, S. 11)

	Schaden	Leistung
Eigenschäden	<ul style="list-style-type: none"> – Wirtschaftliche Schäden durch Betriebsunterbrechung – Kosten der Datenwiederherstellung und System-Rekonstruktion 	<ul style="list-style-type: none"> – Zahlung eines Tagessatzes – Kostenübernahme
Drittschäden	<ul style="list-style-type: none"> – Schadenersatzforderungen von Kunden wegen Datenmissbrauch und/oder Lieferverzug 	<ul style="list-style-type: none"> – Entschädigung und Abwehr unberechtigter Forderungen
Service-Leistungen	<ul style="list-style-type: none"> – IT-Forensik-Experten zur Analyse, Beweissicherung und Schadensbegrenzung – Anwälte für IT- und Datenschutzrecht zur Beratung – PR-Spezialisten für Krisenkommunikation zur Eindämmung des Imageschadens 	<ul style="list-style-type: none"> – Jeweils Vermittlung und Kostenübernahme

Die Grundbausteine einer jeden Cyber-Versicherung ist die finanzielle Absicherung von Eigen und Fremdschäden aus Sicht des Unternehmens. Zu den versicherunten Schäden gehören durch Betriebsunterbrechung entstandene Kosten und Ertragsausfälle sowie Kosten für die Datenwiederherstellung. Darüber hinaus sind Haftpflichtansprüche von Kunden und Lieferanten, aber auch Aufwendungen für IT-Forensik, Krisenkommunikation und Rechtsberatung in Cyber-Policen abgesichert. Die Versicherung soll nicht nur monetäre Verluste ausgleichen, sondern auch mittels Service-Leistungen den Unternehmen mit Expertise zur Seite stehen, um die Schäden im Ernstfall so gering wie möglich zu halten (vgl. Gesamtverband der Deutschen Versicherungswirtschaft 2018, S. 11). Insbesondere durch die Service-Leistungen kann eine Versicherung dem Unternehmen helfen, schon im Vorfeld effektive Maßnahmen zu ergreifen, um Schäden möglicherweise zu verhindern (vgl. Heisz et al. 2017, S. 17).

Die Schwierigkeit besteht darin, den passenden Versicherungsschutz für das eigene Unternehmen zu finden, denn besonders die Definition des Versicherungsfalles spielt eine Rolle. Die hohe Komplexität dieser Produkte resultiert aus den sich ständig ändernden Risikoanforderungen und Schwachstellen. Die Leistungsbauusteine sind für Unternehmen schwer verständlich und aufgrund der Vielseitigkeit der Schadenpotenziale (vgl. Abschn. 21.2.1) passt der offerierte Versicherungsschutz nicht immer zu der nachgefragten Risikoabsicherung (vgl. Flagmeier und Heidemann 2018, S. 10). Durch Cyber-Policen können Schäden nicht unbedingt verhindert werden, jedoch kann eine Kombination aus einem gesamtunternehmerischen Risikomanagement und einer Versicherung einen guten Schutz bieten (vgl. Flagmeier und Heidemann 2018, S. 52).

21.4.4 Marktentwicklung

So wie die Anzahl der Cyber-Attacken ansteigt, wächst auch der Markt für Cyber-Policen seit einigen Jahren stetig. Die nachfrageinduzierte Angebotsausweitung hat nicht nur steigende Prämievolumen zur Folge, sondern auch die Schadenzahlungen steigen an (vgl. Heisz et al. 2017, S. 18). Laut dem Versicherungsmarktreport von Marsh aus dem Frühjahr 2019 gilt die Prämienentwicklung von Cyber-Policen trotz zunehmenden Wettbewerbs als stabil bis leicht steigend. Besonders das Thema „Silent-Cyber“ (vgl. Abschn. 21.4.1) beschäftigt die Versicherungswirtschaft (vgl. Marsh 2019, S. 13). Nicht jedes mögliche Cyber-Risiko wird bisher versichert, da zum Beispiel ein großflächiger systemischer Ausfall einer Infrastruktur die Kapazitäten übersteigen würde. Versicherer arbeiten immer weiter am Verständnis für Cyber-Risiken und deren Schadenpotenziale. Die Schwierigkeit einer adäquaten Bewertung betrifft auch das sich ständig ändernde Umfeld durch die fortschreitende Digitalisierung. Die Versicherer arbeiten mit IT-Spezialisten zusammen, um ihr Know-how mittels eigener Ansätze zu Versicherungsprodukten zu entwickeln. Der Industriever sicherungsmarkt sieht Cyber-Risiken jedoch nicht als unüberwindbar, sondern eher als Chance für Neugeschäft, weswegen die Herausforderung darin besteht, die Komplexität der Produkte zu reduzieren, um eine umfassende, aber auch für Unternehmen verständliche Absicherung bieten zu können (vgl. Golling 2018).

Literatur

- Actual ransom. (2019). Twitter. https://twitter.com/actual_ransom?lang=de. Zugegriffen am 26.07.2019.
- Akamai. (2018). State of the Internet: SecurityWeb attack report.
- Allianz Global Corporate & Specialty SE. (2019). Allianz-Risk-Barometer-2019.
- Biener, C., Eling, M., Matt, A., & Wirfs, J. H. (2015). *Cyber risk: Risikomanagement und Versicherbarkeit*. St. Gallen: Institut für Versicherungswirtschaft der Universität St. Gallen.
- Brokamp, S. (2017). Was ist das eigentlich? Cyberrisiken verständlich erklärt. *AssCompact*, (12/2017), 40.
- Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (2018) „Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie“.
- Bundesamt für Sicherheit in der Informationstechnik. (2019a). Cyber-Sicherheits-Umfrage-Cyber-Risiken & Schutzmaßnahmen in Unternehmen. Allianz für Cyber-Sicherheit.
- Bundesamt für Sicherheit in der Informationstechnik. (2019b). Glossar der Cyber-Sicherheit. https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/cyberglossar_node.html. Zugegriffen am 01.09.2020.
- Cambridge Dictionary. (2020). CYBER- meaning in the Cambridge English Dictionary. Cambridge English Dictionary. <https://dictionary.cambridge.org/de/worterbuch/englisch/cyber>. Zugegriffen am 01.09.2020.
- Dudenredaktion. (o. Jahr). Cyber- I Rechtschreibung, Bedeutung, Definition, Herkunft. Duden. https://www.duden.de/rechtschreibung/cyber_#close-cite. Zugegriffen 27.04.2019
- Flagmeier, W., & Heidemann, J. (2018). *Cyber-Risiken und Versicherungsschutz*. Köln: Wolters Kluwer Deutschland GmbH.
- Gesamtverband der Deutschen Versicherungswirtschaft. (2018) „Cyber-Risiken im Mittelstand“.
- Golling. (2018). Wie versicherbar sind Cyberrisiken? Munich Re. <https://www.munichre.com/topics-online/de/digitalisation/cyber/how-insurable-are-cyber-risks.html>. Zugegriffen am 26.07.2019.
- Heisz, V., Huber, T., Müller, S., Leh Meyer, O., & Richter, A. (2017). „MRIC Executive report – Versicherung als Instrument des Cyber-Risikomanagements“ Munich Risk and Insurance Center.
- Jung, O., Bessler, S., Ceccarelli, A., Zoppi, T., Vasenev, A., Montoya, L., Clarke, T., & Chappell, K. (2016). *Towards a collaborative framework to improve urban grid resilience*. Proceedings of the IEEE International Energy Conference, ENERGYCON 2016, Leuven, Belgien, S. 1–6. <https://doi.org/10.1109/ENERGYCON.2016.7513887>.
- Königs, H.-P. (2017). *IT-Risikomanagement mit System: Praxisorientiertes Management von Informationssicherheits-, IT- und Cyber-Risiken*. Wiesbaden: Springer.
- Marinos, L., & Lourenço, M. (2019). ENISA threat landscape report 2018. European Union Agency for Network and Information Security. <https://doi.org/10.2824/622757>.
- Marsh. (2019). Versicherungsmarktreport 2019 Deutschland.
- Oxford Advanced Learner's Dictionary. (o. J.). Cyber combining form – Definition, pictures, pronunciation and usage. Oxford Learner's Dicitonary. <https://www.oxfordlearnersdictionaries.com/definition/english/cyber?q=cyber>. Zugegriffen am 01.09.2020.
- Pohlmann, F., & Fritzen, R. (2015). Distributed Denial of Service Attacks (DDoS). (2). S. 60–65.
- Reynolds, M. (2017). Ransomware attack hits 200,000 computers across the globe. <https://www.newscientist.com/article/2130983-ransomware-attack-hits-200000-computers-across-the-globe/>. Zugegriffen am 17.05.2019.
- RiskNET. (2019). Glossar – RiskNET – The Risk Management Network. https://www.risknet.de/wissen/glossar/?tx_a21glossary_pi1%5Bchar%5D=Risiko%20%28Definition%29&tx_a21glossary_pi1%5Bcontroller%5D=Glossary&cHash=c852759d624c4cd2b0204a1f9ad11f7e. Zugegriffen am 01.09.2020.

- Siebert, R. (2019). Wirtschaft Stellungnahme zum „silent cyber“ – Thema. GVNW Gesamtverband der versicherungsnehmenden. <https://www.gvnw.de/news/detail/stellungnahme-zum-silent-cyber-thema>. Zugegriffen am 26.07.2019.
- Symantec. (2019). Internet security threat report (24).
- Thommen, J. (2019). Definition: Anspruchsgruppen. Gabler Wirtschaftslexikon. <https://wirtschaftslexikon.gabler.de/definition/anspruchsgruppen-27010>. Zugegriffen am 26.07.2019.
- Tittko, H. (2018). Ansätze zur Abgrenzung traditioneller betrieblicher Versicherungen von Cyber-Versicherungen aktueller Prägung, Gesamtverband der versicherungsnehmenden Wirtschaft e. V. *Die VersicherungsPraxis*, 8, 29–30.
- Wolke, T. (2009). *Risikomanagement*. München: de Gruyter.
- Wrede, D., Freers, T., & Graf von der Schulenberg, J. (2019). *Herausforderungen und Implikationen für das Cyber-Risikomanagement sowie die Versicherung von Cyberrisiken – Eine empirische Analyse*. Springer. <https://doi.org/10.1007/s12297-018-0425-2>.

Andreas Walz ist seit 2011 Chief Information Security Officer (CISO) der Talanx Gruppe und Leiter der Group Security. Er ist zertifizierter IT Sicherheitsbeauftragter und arbeitete mehrere Jahre als Leiter Information Risk- und Prozess Management. Nach seinem Mathematik und Informatik Studium arbeitete Herr Walz zunächst als Leiter Benutzerservice für die E&L, spätere AXA-Leben. Nebenbei gibt er zahlreiche Vorträge aus dem Bereich Informationssicherheit auf verschiedenen Veranstaltungen und an Lehreinrichtungen.

Jörg Klemens ist seit dem 01.01.2019 Security Architect innerhalb der Group Security des Talanx Konzerns. Nach erfolgreichem Studium der Wirtschaftsinformatik arbeitete er zunächst als SAP Basis Administrator für den Gerling Konzern, heute Talanx. Im Anschluss leitete Herr Klemens den Bereich Identity- und Accessmanagement innerhalb der Talanx Systeme AG. Seit mehr als 15 Jahren unterrichtet er zudem Wirtschaftsmathematik, wissenschaftliches Arbeiten und betriebliche Informationssysteme an der FHDW (Fachhochschule der Wirtschaft).

Romina Röpke studierte Insurance and Finance an der Hochschule RheinMain in Wiesbaden. Im Anschluss absolvierte sie das Masterstudium Risk & Insurance am Institut für Versicherungswesen der Technischen Hochschule Köln. Während des Masterstudiums arbeitete sie als Werkstudentin bei ASSEKURATA Assekuranz Rating-Agentur GmbH, wo sie nach erfolgreichem Abschluss ihres Studiums in die Position der Junior Analystin übernommen wurde.



Warranty & Indemnity-Versicherung bei der Unternehmenstransaktion

22

Carolin van Straelen, Bernd Dreier und Jannik Revers

Zusammenfassung

Seit einigen Jahren werden bei Unternehmenstransaktionen Risiken aus Garantien und Freistellungsverpflichtungen des Verkäufers zugunsten des Käufers immer häufiger durch sogenannte Warranty & Indemnity-Versicherungen (W&I-Versicherungen) abgesichert. Dieser Beitrag befasst sich mit den Grundlagen, den Vorteilen und Motiven sowie dem Prozess für den Abschluss einer solchen W&I-Versicherung bei der Unternehmenstransaktion.

22.1 Ausgangssituation

Die W&I-Versicherung kommt sowohl bei einem Asset Deal, bei dem die Vermögensgegenstände des Zielunternehmens an den Käufer veräußert werden, als auch bei einem Share Deal, der auf die Veräußerung der Gesellschaftsanteile an dem Zielunternehmen gerichtet ist, zur Anwendung. Anknüpfungspunkt ist in beiden Fällen der Unternehmenskaufvertrag und insbesondere die darin vereinbarten Garantien und Freistellungsverpflichtungen.

Die Verfasser dieses Beitrages handeln ausschließlich als Privatpersonen. Die in diesem Beitrag vertretenen Ansichten spiegeln nicht die Standpunkte der AIG Europe SA oder verbundener Unternehmen wider.

C. van Straelen (✉) · B. Dreier
AIG Europe S. A., München, Deutschland
E-Mail: Carolin.Vanstraelen@aig.com; Bernd.Dreier@aig.com

J. Revers
TH Köln, Institut für Versicherungswesen, Köln, Deutschland
E-Mail: jannikrevers@web.de

22.1.1 Unternehmenskaufvertrag und Garantien

Üblicherweise vereinbaren die Parteien in Unternehmenskaufverträgen bestimmte Garantien, für deren Richtigkeit der Verkäufer gegenüber dem Käufer haftet, sowie ggf. Freistellungen, unter denen der Verkäufer bei Vorliegen der entsprechenden Voraussetzungen gegenüber dem Käufer verpflichtet ist, ihn bis zu bestimmten Haftungshöchstbeträgen freizustellen. Diese Garantien sollen den Käufer trotz umfassender, systematischer Untersuchung und Prüfung des Unternehmens (sogenannte Due Diligence) vor unbekannten Risiken schützen bzw. im Falle von Freistellungsverpflichtungen eine Übernahme bereits bekannter Risiken durch den Verkäufer bewirken (vgl. Franz und Keune 2013, S. 1371; vgl. Sommer et al. 2019, S. 118). Inhalt und Umfang solcher Garantien und/oder Freistellungen hängen von den Besonderheiten der Transaktion und der Transaktionsstruktur ab. Regelmäßig wird die Haftung des Verkäufers durch Vereinbarung bestimmter Bagatellgrenzen, Mindestbeträge und Haftungsgrenzen begrenzt.

Eine wesentliche Herausforderung ist die adäquate Risikoverteilung zwischen den Parteien. Während der Käufer eine möglichst weitreichende Haftung des Verkäufers verhandeln will, liegt es im Interesse des Verkäufers, seine Haftung so weit wie möglich einzuschränken (vgl. Hoenig und Klingen 2016, S. 1244; vgl. Haberstock 2008, S. 29 f.; vgl. Jakobs und Franz 2014, S. 659; vgl. Grossmann und Mönnich 2003, S. 708).

In bestimmten Konstellationen ist der Verkäufer trotz Haftungsbeschränkungen nicht bereit oder in der Lage, Garantien und/oder Freistellungen abzugeben. Dies ist etwa der Fall bei Finanzinvestoren auf Verkäuferseite, die nicht in das operative Geschäft des Zielunternehmens eingebunden sind und deren Veräußerungserlöse aus der Transaktion direkt an die Investoren ausgeschüttet werden (vgl. Franz und Keune 2013, S. 1371 f.; vgl. Jakobs und Franz 2014, S. 659; vgl. Weitnauer 2016, S. 413). Ebenso wird ein Insolvenzverwalter regelmäßig kaum Garantien abgeben, da er zum einen das von ihm verwaltete Unternehmen häufig erst wenige Wochen kennt und kaum verlässliche Zusagen zum Zustand des Unternehmens machen kann (vgl. FAZ vom 12.06.2019, Verkauf vom Verwalter – Versicherung für Unternehmenskauf bei Insolvenz) und zum anderen bestrebt ist, die Insolvenzmasse von langfristigen Garantiezusagen, die zusätzliche Masseverbindlichkeiten darstellen, freizuhalten (vgl. Jakobs und Franz 2014, S. 659 und 660).

Aber auch der Familienunternehmer, der seine Erwerbsgrundlage veräußert, oder der strategische Marktteilnehmer, der zum Beispiel eine Unternehmensparte verkauft, möchten spätere Haftungsfälle vermeiden (vgl. Hoenig und Klingen 2016, S. 1244; vgl. Hensel und Namislo 2018, S. 1475). Gleches gilt in Konstellationen, in denen die Altgesellschafter oder das Managementteam weiterhin am Zielunternehmen beteiligt bleiben und Haftungsfälle im eigenen Gesellschafterkreis ausgetragen werden müssen (vgl. Jakobs und Franz 2014, S. 659; vgl. Hensel und Namislo 2018, S. 1475).

22.1.2 Garantieverletzungen

Garantien des Verkäufers im Hinblick auf das Zielunternehmen werden regelmäßig nicht als Gewährleistungen im Sinne des Bürgerlichen Gesetzbuches vereinbart, da die Regelungen des Bürgerlichen Gesetzbuches keinen Zuschnitt auf die einzelne Transaktion erlauben (vgl. Klapper 2016, S. 42 und 45; Hörmann, in: P+P Festschrift 2008, S. 135 und 139). Insbesondere die gesetzlich angeordnete Rechtsfolge der Rückabwicklung der Transaktion ist zudem wenig praktikabel (vgl. Hörmann 2008, S. 135 und 139). Garantien werden vielmehr unter Ausschluss des sogenannten kaufrechtlichen Gewährleistungsrechtes als selbstständige Garantieversprechen abgegeben und die Rechtsfolgen von Garantieverletzungen bzw. Freistellungssachverhalten ausschließlich im Unternehmenskaufvertrag geregelt.

Zur Sicherung etwaiger Ansprüche des Käufers wird häufig vereinbart, dass ein Teil des Kaufpreises als Sicherheit einbehalten oder auf ein Treuhandkonto gezahlt und erst nach Ablauf der für die Garantien oder Freistellungen vereinbarten Verjährungsfristen an den Verkäufer ausgezahlt wird (vgl. Jakobs und Franz 2014, S. 659 und 660). Weitere gebräuchliche Sicherungsmittel sind die Abgabe einer (Bank-)Bürgschaft durch eine Bank als Sicherungsgeber sowie die Patronatserklärung bzw. der Schuldbeitritt eines Mutterunternehmens. Diese klassischen Sicherungsmittel sind jedoch für den Verkäufer unattraktiv bzw. stehen teilweise gar nicht erst zur Verfügung (vgl. Jakobs und Franz 2014, S. 659 und 661). So erhält der Verkäufer im Fall des Kaufpreiseinbehalts bzw. der Treuhandlösung den vollen Kaufpreis ggf. erst nach Jahren, während die Patronatserklärung bzw. der Schuldbeitritt regelmäßig nur in Konzernstrukturen in Betracht kommen (vgl. Jakobs und Franz 2014, S. 659 und 661). (Bank-)Bürgschaften wiederum belasten die Kreditlinie des Verkäufers und bergen bei einer Bürgschaft auf erstes Anfordern das Risiko einer unberechtigten Inanspruchnahme durch den Käufer (vgl. Grossmann und Mönnich 2003, S. 708 und 709).

22.2 Grundlagen der W&I-Versicherung

22.2.1 Einleitung

Vor diesem Hintergrund hat sich eine Praxis etabliert, Schäden, die aus der Verletzung von Garantien sowie infolge eines eine Freistellung auslösenden Ereignisses in Unternehmenskaufverträgen entstehen, durch hierauf spezialisierte Versicherer abzusichern (sogenannte Warranty & Indemnity Insurance, Warranty & Indemnity Versicherung und im Folgenden: W&I-Versicherung). Der Versicherer wird dabei nicht selbst Partei des Unternehmenskaufvertrages. Solche W&I-Versicherungen haben ihren Ursprung im anglo-amerikanischen Raum. Inzwischen sind sie auch in Europa, vorwiegend in Großbritannien und Skandinavien, aber auch in der DACH-Region, verbreitet (vgl. Froneberg und Dannemann 2017, S. 21; vgl. Hoger und Baumann 2017, S. 811; vgl. Jakobs und Franz 2014, S. 659; vgl. AIG

2016). In Europa werden etwa 35 Prozent aller M&A-Transaktionen von einer W&I-Versicherung begleitet (vgl. Latham & Watkins, 6th Annual Private M&A Market Study 2019), wobei der Anteil bei Transaktionen mit einem Private Equity Fonds als Verkäufer sogar etwa 48 Prozent beträgt (vgl. Latham & Watkins 2019). Bei einem Transaktionsvolumen von über 100 Millionen Euro sind es sogar etwa 50 Prozent (vgl. CMS European M&A Study 2020). Mit der W&I-Versicherung können Unternehmenstransaktionen aller Branchen und Industriezweige abgesichert werden. Die Transaktionsvolumina reichen insgesamt von 15 Millionen bis drei Milliarden Euro (vgl. Froneberg et al. 2017, S. 216).

Durch den Abschluss einer W&I-Versicherung verringern sich einerseits das Haftungsrisiko des Verkäufers und andererseits das Durchsetzungsrisiko von Ansprüchen des Käufers gegenüber dem Verkäufer. Zugleich besteht die Möglichkeit, als sogenannte synthetische Versicherung bestimmte Tatbestandsmerkmale und/oder Rechtsfolgen für die Zwecke der Versicherungspolice zugunsten des Versicherungsnehmers anzupassen, etwa die Nichtberücksichtigung von Kenntnisqualifikationen des Verkäufers („Knowledge Scrape“), die Verjährungsfristen oder die Haftungsgrenzen (vgl. Klingenheben 2016, S. 10).

Vom Versicherungsschutz einer W&I-Versicherung ausgenommen sind bekannte und sich sicher realisierende Sachverhalte, die Verletzung von in die Zukunft gerichteten Garantien, der Eintritt künftiger Ereignisse, etwa die Erzielung bestimmter Unternehmensergebnisse nach Vollzug der Transaktion sowie sonstige vertragliche Verpflichtungen oder Bußgelder (vgl. Hensel und Namislo 2018, S. 1475 und 1477; vgl. Daghles und Haßler 2016, S. 455 und 456; vgl. Jakobs und Franz 2014, S. 659 ff.; vgl. Hoger und Baumann 2017, S. 811 und 812; vgl. Grossmann und Mönnich 2003, S. 708 und 711). Für bekannte Risiken aus Steuer- oder Umweltsachverhalten oder gerichtlichen Streitigkeiten (sogenannte Litigation Buy-outs) sowie Eventualverbindlichkeiten können darüber hinaus Spezialversicherungen abgeschlossen werden, die ebenfalls immer mehr an Bedeutung gewinnen (vgl. Grädler et al. 2018, S. 464 und 465; vgl. Froneberg und Dannemann 2017, S. 26; vgl. Oberbracht 2015, S. 26). Die Prüfung der Versicherbarkeit einzelner Risiken durch den Versicherer setzt eine fundierte und umfassende Due-Diligence-Prüfung des Käufers und einen hinreichenden Offenlegungsprozess des Verkäufers voraus (vgl. Klingenheben 2016, S. 10 und 12; vgl. Rasner et al. 2018, S. 24 und 25).

Die wesentlichen Versicherungsbedingungen und die zu zahlende Prämie einer solchen W&I-Versicherung sind stark marktgetrieben und hängen vom Deckungsumfang des Versicherungsschutzes, der Versicherungsdauer und dem vertraglich vereinbarten Selbstbehalt ab (vgl. Sommer et al. 2019, S. 118 und 119; vgl. Klingenheben 2016, S. 10). In der Praxis sind Deckungssummen in der Bandbreite von 10 bis 50 Prozent des Unternehmenswertes (Enterprise Value) bei einem Selbstbehalt zwischen 0,25 Prozent und einem Prozent zu beobachten (vgl. Giessen und Lüttges 2019, S. 331; vgl. Hensel und Namislo 2018, S. 1475 und 1477; vgl. Grädler et al. 2018, S. 464 und 465; vgl. Hoenig und Klingen 2016, S. 1244 und 1247). Bei Immobilientransaktionen, aber auch bei Unternehmenskäufen, gibt es eine zunehmende Tendenz der Versicherer, den Selbstbehalt entfallen zu lassen (sogenanntes „tipping to nil“ oder „nil-recourse“) (vgl. Grädler et al. 2018, S. 464 und 465; vgl. Rasner et al. 2018, S. 24; vgl. Fairhurst und Treagus 2016, S. 10 f.).

Die W&I-Versicherung kann entweder durch den Verkäufer (Verkäuferpolice) oder den Käufer (Käuferpolice) als Versicherungsnehmer abgeschlossen werden.

22.2.2 Verkäuferpolice

Die Verkäuferpolice ist als Vermögensschadenhaftpflichtversicherung im Sinne der §§ 100 ff. VVG zu qualifizieren (vgl. Wiegand 2017, § 84 Rn 6; vgl. Metz 2010, S. 813 und 814; vgl. Daghles und Haßler 2016, S. 455). Sie deckt das Risiko des Verkäufers ab, für den Fall einer Verletzung von Garantien im Unternehmenskaufvertrag in Anspruch genommen zu werden. Der Verkäufer als Versicherungsnehmer der W&I-Versicherung hat im Schadensfall einen Anspruch gegen den Versicherer auf Freistellung von Ansprüchen des Käufers (vgl. Daghles und Haßler 2016, S. 455; vgl. Hiort 2012, S. 127 und 128). Zudem übernimmt der Versicherer die rechtliche Verteidigung gegen unbegründete Ansprüche des Käufers.

Der Käufer muss seine Ansprüche wegen Garantieverletzungen bzw. im Falle des Eintritts eines auslösenden Ereignisses zunächst gegen den Verkäufer geltend machen und ggf. (abhängig von den Regelungen in der Versicherungspolice) rechtskräftig (schieds-)gerichtlich feststellen lassen. Anschließend kann der Verkäufer im Rahmen der Deckung unter der Versicherungspolice Rückgriff bei dem Versicherer nehmen (vgl. Grädler et al. 2018, S. 464). Eine direkte Inanspruchnahme des Versicherers durch den Käufer ist nur möglich, wenn der Versicherer einer Abtretung des Versicherungsanspruchs zustimmt (vgl. Hiort 2012, S. 127 und 128). Ein wesentlicher Nachteil der Verkäuferpolice besteht darin, dass die Haftung des Verkäufers nicht herabgesetzt werden kann (vgl. Froneberg et al. 2017, S. 216 und 217). Für Schäden, die nicht von der Versicherungspolice gedeckt sind, haftet der Verkäufer weiterhin gegenüber dem Käufer. Der Verkäufer trägt somit das Risiko etwaiger Deckungslücken zwischen der Versicherungspolice und dem Unternehmenskaufvertrag. Zudem entfällt der Versicherungsschutz für vorsätzliche oder grob fahrlässige Falschangaben des Verkäufers sowie Angaben „ins Blaue hinein“ bei Abgabe der Garantien im Unternehmenskaufvertrag.

Abb. 22.1 veranschaulicht zusammengefasst die Verkäuferpolice.

Während bei den ersten abgeschlossenen W&I-Versicherungen der Verkäufer Versicherungsnehmer war, werden W&I-Versicherungen inzwischen weit überwiegend vom Käufer abgeschlossen (vgl. Wiegand 2017, § 84 Rn 1 f.; vgl. Grädler et al. 2018, S. 464; vgl. Giessen und Luttgess 2018, S. 647).

22.2.3 Käuferpolice

Bei der Käuferpolice schließt der Käufer die Versicherungspolice mit dem Versicherer ab. Die Käuferpolice ist nach herrschender Meinung eine Vermögenseigenschadenversicherung, die den Käufer vor bestimmten Schäden des eigenen Vermögens schützen soll (vgl.



Abb. 22.1 Verkäuferpolice. (Quelle: eigene Darstellung in Anlehnung an AIG 2017, S. 8)

Daghles und Haßler 2016, S. 455; vgl. Hensel und Namislo 2018, S. 1475; vgl. Jakobs und Franz 2014, S. 659 und 663; vgl. Metz 2010, S. 813 und 814; vgl. Kränzlin et al. 2013, S. 2315, die die Käuferpolice als Betriebsunterbrechungsversicherung einordnen; vgl. Wiegand 2017, § 84 Rn 6, der die Käuferpolice als Vertrag sui generis einordnet). Der Käufer kann sich im Schadensfall direkt an den Versicherer wenden, ohne den Verkäufer aus dem Unternehmenskaufvertrag in Anspruch nehmen zu müssen (vgl. Daghles und Haßler 2016, S. 455; vgl. Hiort 2012, S. 129; vgl. Oberbracht 2015, S. 26 und 27). Der Anspruch besteht unabhängig von der Haftung im Unternehmenskaufvertrag. Verkäufer bestehen in der Praxis deshalb häufig darauf, ihre Haftung auf einen Euro zu begrenzen (vgl. Kugler und Thiele 2016, S. 32 und 33).

Zudem muss (im Gegensatz zur Verkäuferpolice) der Anspruch nicht rechtskräftig festgestellt werden. Es genügt, dass der Käufer die Verletzung einer Garantie oder den Eintritt eines eine Freistellung auslösenden Ereignisses und den Schaden gegenüber dem Versicherer nachweist (vgl. Daghles und Haßler 2016, S. 455 und 456; vgl. Hasselbach und Reichel 2005, S. 377 und 378; vgl. Sommer et al. 2019, S. 118 und 119).

Weiter entfällt der Anspruch des Käufers im Falle von Vorsatz oder grober Fahrlässigkeit des Verkäufers nicht, da nicht dem Käufer als Versicherungsnehmer, sondern dem Verkäufer ein Fehlverhalten vorzuwerfen ist (vgl. Daghles und Haßler 2016, S. 455; vgl. Jakobs und Franz 2014, S. 659 und 664). Führt jedoch der Käufer den Versicherungsfall vorsätzlich oder grob fahrlässig herbei, ist der Versicherer berechtigt, seine Leistung (anteilig) zu verweigern. Dies kann insbesondere bei kollusivem Zusammenwirken von Verkäufer und Käufer zum Nachteil des Versicherers der Fall sein (vgl. Jakobs und Franz 2014, S. 659 und 664).

Abb. 22.2 veranschaulicht zusammengefasst die Käuferpolice.

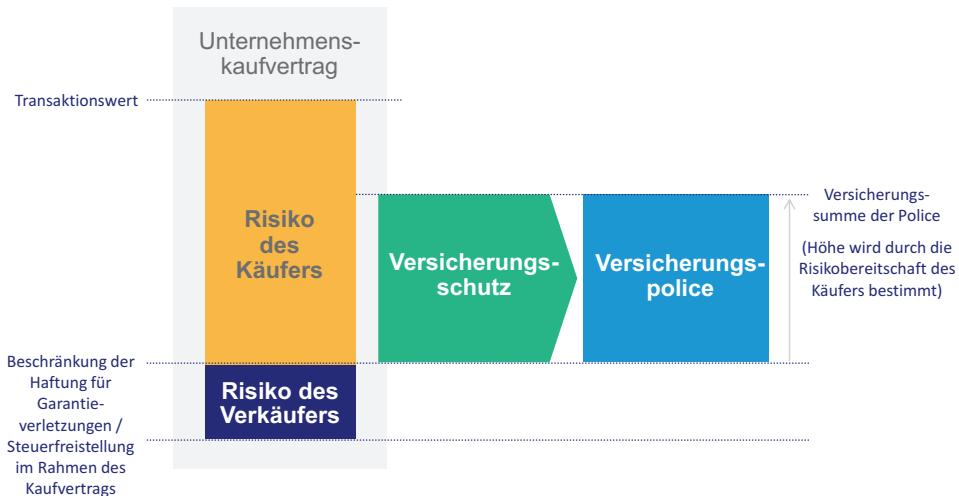


Abb. 22.2 Käuferpolize. (Quelle: eigene Darstellung in Anlehnung an AIG 2017, S. 9)

22.3 „Seller Buyer Flip“

In der Praxis beginnt häufig der Verkäufer die Verhandlungen mit dem Versicherer auf Grundlage der dem Versicherer seitens des Verkäufers zur Verfügung gestellten Informationen. Anschließend leitet er den Prozess auf den Käufer bzw. eine kleine Anzahl aussichtsreicher Bieter im Rahmen von Auktionsprozessen über und der Käufer bzw. diese Bieter führen jeweils mit den präferierten Versicherern oder auch zur Wahrung der Vertraulichkeit mit so genannten Chinese Walls mit unterschiedlichen Teams des gleichen Versicherers die Verhandlungen zu Ende. Der Käufer bzw. der erfolgreiche Bieter schließt dann die Versicherungspolice als Versicherungsnehmer mit dem Versicherer ab (sogenannter „Seller Buyer Flip“ oder „Stapled Insurance“) (vgl. Daghles und Haßler 2016, S. 455 und 456; vgl. Kaufhold 2016, S. 394 und 395; vgl. Giessen und Lüttges 2018, S. 647 und 648). Der „Seller Buyer Flip“ erfolgt frühestens nach Erhalt der unverbindlichen Einschätzungen (sogenannte „non-binding indications“, vgl. hierzu Abschn. 22.5) durch die Versicherer und spätestens nach Vorliegen einer ausverhandelten Police mit dem Verkäufer. Sofern der Verkäufer nur Gebote von Bietern akzeptiert, die die ausverhandelte Versicherungspolice übernehmen und Anpassungen nur anhand von neuen Informationen oder Informationen, die dem Versicherer auf Verkäuferseite nicht vorlagen, vornimmt, wird von einer „Hard-stapled Insurance“ gesprochen. Diese kommt jedoch in der Praxis sehr selten vor.

Der „Seller Buyer Flip“ kommt vor allem bei kompetitiven Auktionsprozessen zum Einsatz und ist insbesondere bei Finanzinvestoren, die ein Investment beenden, beliebt, weil es die Transaktionssicherheit und Geschwindigkeit erhöht (vgl. Froneberg et al. 2017, S. 216 und 217).

22.4 Vorteile und Motive einer W&I-Versicherung

Die W&I-Versicherung kann auf unterschiedliche Weise in einer Transaktion zum Einsatz kommen.

Die Verhandlungen zwischen den Parteien können zu Beginn ohne eine W&I-Versicherung starten. Falls es zu einem Verhandlungsstillstand kommt, etwa, weil die Parteien sich nicht auf Inhalt und Umfang der vom Verkäufer unter dem Unternehmenskaufvertrag abzugebenden Garantien und/oder Freistellungsverpflichtungen einigen können, kann die W&I-Versicherung dazu eingesetzt werden, diesen Interessenkonflikt zu überbrücken, sogenanntes „Bridging the Gap“ (vgl. Grädler et al. 2018, S. 464 und 465; vgl. Lips o. J.). Wenn der Verkäufer zum Beispiel lediglich bereit ist, eine Haftung in Höhe von fünf Prozent des Transaktionsvolumens zu akzeptieren, der Käufer aufgrund interner (im Fall von Kapitalanlagegesellschaften im Immobilienbereich möglicherweise auch regulatorischer) Anforderungen aber auf einen Haftungshöchstbetrag von 30 Prozent des Transaktionsvolumens oder mehr angewiesen ist, kann ein Verhandlungsstillstand oder gar ein Scheitern der Transaktion durch eine Versicherungslösung abgewendet werden (vgl. Froneberg et al. 2017, S. 216 und 217).

Der Verkäufer kann den Verkaufsprozess aber auch zusammen mit einer W&I-Versicherung aufsetzen und die Garantien im Unternehmenskaufvertrag von vornherein mit dem Versicherer auf seine Versicherbarkeit abstimmen (vgl. AIG 2017, S. 12 f.). Auf diese Weise kann der Verkäufer die Garantien im Unternehmenskaufvertrag auf die Versicherungspolice abstimmen, um Haftungslücken und damit eine spätere Inanspruchnahme durch den Käufer auszuschließen (vgl. Franz und Keune 2013, S. 1371 f.). Gleichzeitig wird der Haftungshöchstbetrag des Verkäufers auf einen Euro festgesetzt. Dies ist insbesondere für Finanzinvestoren attraktiv, denen damit ein „Clean Exit“ gelingt (vgl. Grädler et al. 2018, S. 464 und 465; vgl. Klingenberg 2016, S. 10). Aber auch ein Insolvenzverwalter wird so in die Lage versetzt, Garantien gegenüber dem Käufer abzugeben, ohne dass er eine Belastung der Insolvenzmasse mit Haftungsrisiken fürchten muss.

Der Abschluss einer W&I-Versicherung kann auch dann sinnvoll sein, wenn beide Parteien nach Vollzug der Transaktion weiter zusammenarbeiten möchten, etwa im Rahmen eines Joint Ventures oder einer Kundenbeziehung (vgl. Fingerhuth et al. 2016; vgl. Oberbracht 2015, S. 26 und 27). Gleches gilt, wenn Altgesellschafter oder das Managementteam nach Abschluss der Transaktion am Unternehmen beteiligt bleiben. Indem sich etwaige Schadensersatzansprüche gegen den Versicherer richten, bleibt die Beziehung zwischen Verkäufer und Käufer unbelastet (vgl. Werlen und Mannsdorfer 2013, S. 398 f.).

Aus Sicht des Käufers stellt die W&I-Versicherung einen weiteren Nutzen dar, wenn zu befürchten ist, dass es einem finanziell schwachen Verkäufer oder einer für die Zwecke der Transaktion gegründete Zweckgesellschaft an der erforderlichen Liquidität fehlen wird, um Schadensersatz für die Verletzung vertraglicher Garantien zu leisten bzw. den Käufer freizustellen (vgl. Franz und Keune 2013, S. 1371; vgl. Hoenig und Klingenberg 2016, S. 1244). Der Käufer erhält hierdurch einen solventen Schuldner.

Die W&I-Versicherung tritt häufig an die Stelle anderer Sicherungsmittel. Durch den Abschluss einer W&I-Versicherung ist dem Sicherungsbedürfnis des Käufers ausreichend Rechnung getragen. Der Verkäufer muss dann keine weiteren Sicherungsgeber zur Verfügung stellen und eine Hinterlegung des Kaufpreises zu in der Regel niedrigen Zinsen auf einem Treuhandkonto ist entbehrlich. Vielmehr hat der Verkäufer sofortigen Zugriff auf den vollen Kaufpreis und muss keine Rückstellungen für etwaige Verbindlichkeiten bilden (vgl. Hensel und Namislo 2018, S. 1475; vgl. Sommer et al. 2019, S. 118 und 119; vgl. Oberbracht 2015, S. 26 und 27; vgl. Hermann, 2015, § 39 Rn 151).

Vor allem in den Anfangsjahren wurde die W&I-Versicherung in Bieterverfahren dazu genutzt, das eigene Angebot gegenüber den Angeboten der anderen Bieter attraktiver zu gestalten, indem sie von vornherein die Bereitschaft zeigten, eine W&I-Versicherung abzuschließen (sogenanntes „Sweetening the Bid“). Spiegelbildlich konnten Verkäufer durch die Abgabe umfangreicher Garantien und Freistellungsverpflichtungen bessere Angebote erzielen (sogenanntes „Dress up the Bride“) (vgl. Werlen und Mannsdorfer 2013, S. 398 f.).

Die vorgenannten Motive zum Einsatz der W&I-Versicherung treten jedoch mit steigender Akzeptanz dieser Versicherungslösung im Markt in den Hintergrund und im deutschsprachigen Raum kann zumindest für den deutschen Markt inzwischen der Einsatz oder zumindest die Einholung von Angeboten zum Abschluss einer W&I-Versicherung als gängige Praxis bezeichnet werden.

Tab. 22.1 zeigt die Vorteile der W&I-Versicherung aus Käufer- und Verkäufersicht.

Tab. 22.1 Vorteile der W&I-Versicherung aus Käufer- und Verkäufersicht

Vorteile für den Käufer	Vorteile für den Verkäufer
<ul style="list-style-type: none"> – Vermeidung langwieriger Garantieverhandlungen bzw. Möglichkeit zur Überbrückung von Differenzen zwischen den Parteien – Langfristige Sicherung von Geschäftsverbindungen durch Vermeidung von Streitigkeiten zwischen den Parteien – Verlagerung von Haftungsrisiken – Erhöhung der Attraktivität des Angebots in Auktionsverfahren z. B. durch erweiterte Garantien im Auktionsverfahren („Sweetening the Bid“) – Längere Verjährungsfristen und höhere Haftungsgrenzen – Absicherung gegen Insolvenzrisiko des Verkäufers 	<ul style="list-style-type: none"> – Vermeidung langwieriger Garantieverhandlungen bzw. Möglichkeit zur Überbrückung von Differenzen zwischen den Parteien – Langfristige Sicherung von Geschäftsverbindungen durch Vermeidung von Streitigkeiten zwischen den Parteien – Vermeidung nachvertraglicher Ansprüche („Clean Exit“) – Verzicht auf Treuhandkonto, Einbehälte des Kaufpreises, Ausfallgarantiegeber und Bankbürgschaften zur Sicherung von Ansprüchen – Volle Ausschüttung des Veräußerungserlöses an Gesellschafter/Investoren unmittelbar nach Transaktionsende – Erzielung besserer Angebote

22.5 Abschluss einer W&I-Versicherung

In einem ersten Schritt sprechen in der Regel die Berater des Verkäufers bzw. des Käufers auf anonymer Basis einen (ggf. auch mehrere) auf W&I-Versicherungen spezialisierten Versicherungsmakler an. In welcher Phase der Unternehmenstransaktion eine solche erste Ansprache erfolgt, hängt im Einzelfall von den für die Inanspruchnahme einer W&I-Versicherung ausschlaggebenden Motiven ab. In einem Auktionsprozess etwa erfolgt die Ansprache bereits in der Anfangsphase der Unternehmenstransaktion und zumeist auf der Verkäuferseite, der den Prozess später auf den Käufer überleiten möchte. Können sich die Parteien etwa auf den Umfang einzelner Garantien nicht einigen, erfolgt die Ansprache hingegen zumeist in einem fortgeschrittenen Stadium, teilweise auch erst kurz vor der Unterzeichnung des Unternehmenskaufvertrages.

Nach der Mandatierung erhält der Versicherungsmakler den Entwurf des Unternehmenskaufvertrages, einschließlich der Garantien und Freistellungsverpflichtungen, sowie weitere Informationen zur Transaktion, zum Zielunternehmen und zum Versicherungsschutz (gewünschte Deckungssumme, Selbstbehalt, Laufzeit etc.). Diese leitet er auf vertraulicher Basis an mehrere in Frage kommende Versicherer weiter. Die Versicherer werten die ihnen zur Verfügung gestellten Informationen aus und geben unverbindliche Einschätzungen (sogenannte „non-binding indications“) zu den Kosten und dem Umfang des Versicherungsschutzes ab. Der Versicherungsmakler prüft diese Angebote und trifft gegebenenfalls eine Vorauswahl (vgl. Daghles und Haßler 2016, S. 455 und 456). Im weiteren Prozess agiert er als Koordinator zwischen den Beteiligten der Unternehmenstransaktion und dem Versicherer.

Sobald sich der Verkäufer bzw. der Käufer für einen Versicherer entschieden haben, beginnt das sogenannte „Underwriting“. Der Versicherer erhält Zugang zum Datenraum und je nachdem, ob der Prozess von der Verkäufer- oder der Käuferseite eingeleitet wurde, die Factbooks des Verkäufers bzw. die Due-Diligence-Reports des Verkäufers bzw. des Käufers. Der Versicherer wertet die ihm zur Verfügung gestellten Informationen aus und stellt gegebenenfalls Rückfragen, soweit Bereiche nicht oder nicht hinreichend darstellt wurden. Diese Rückfragen werden zunächst vom Verkäufer bzw. Käufer und den Beratern schriftlich gestellt und sodann zum Beispiel in einem gemeinsamen Telefonat (sogenannter „Underwriting Call“) erläutert und diskutiert. Anschließend erstellt der Versicherer auf dieser Grundlage einen Entwurf der Versicherungspolice mit den entsprechenden Deckungspositionen. Diese Versicherungspolice wird sodann zwischen dem Versicherer und dem Käufer unter Beteiligung des Versicherungsmaklers und der Berater des Käufers abschließend verhandelt. Auf Seiten der Versicherer agieren zumeist professionelle, spezialisierte Teams, um ein zügiges und effizientes Underwriting zu gewährleisten.

In der Regel zeitgleich mit der Unterzeichnung des Unternehmenskaufvertrages wird auch die W&I-Versicherung abgeschlossen. Anschließend muss der Käufer als Versicherungsnehmer bestätigen, dass ihm weder bei Unterzeichnung noch bei Vollzug des Unternehmenskaufvertrages Garantieverletzungen bekannt waren, die zu einem Versicherungsfall

führen können (sogenannte „No Claims Declaration“). Hintergrund hierfür ist, dass der Käufer keinen Versicherungsschutz für ihm bekannte bzw. arglistig verschwiegene Garantieverletzungen unter der W&I-Versicherung erhalten soll.

22.6 Fazit

Anknüpfungspunkt für die W&I-Versicherung ist der Unternehmenskaufvertrag und vor allem die darin zwischen dem Verkäufer und dem Käufer vereinbarten Garantien und Freistellungsverpflichtungen.

Es sind grundsätzlich zwei Formen der W&I-Versicherung zu unterscheiden: die Verkäuferpolice und die Käuferpolice. In der Praxis werden weit überwiegend Käuferpolices geschlossen. Nur etwa ein Prozent der geschlossenen W&I-Versicherungspolices sind Verkäuferpolices. Teilweise nimmt zunächst der Verkäufer die Verhandlungen mit dem Versicherer auf und leitet den Prozess erst zu einem späteren Zeitpunkt auf den Käufer über, sogenannter „Seller Buyer Flip“.

Die W&I-Versicherung ist aus Käufer- aber auch aus Verkäufersicht ein sinnvolles Instrument zur Verringerung von Interessengegensätzen und zur Risikoverteilung im Rahmen von Unternehmenstransaktionen.

Die Vorteile einer W&I-Versicherung sind bei Verkäufern und Käufern inzwischen gleichermaßen anerkannt. Seit einigen Jahren besteht die steigende Tendenz, diese Interessengegensätze und Risiken gegen Zahlung einer Prämie mittels einer W&I-Versicherung auf einen Versicherer zu übertragen, der für die Abwicklung etwaiger Ansprüche des Käufers einsteht.

Mit der kontinuierlich steigenden Anzahl von Transaktionen, für die eine W&I-Versicherung abgeschlossen wird, steigt auch der Wettbewerb unter den Versicherern. Der größere Wettbewerb unter den Versicherern hat wiederum zu sinkenden Prämien, zu einem professionelleren und schnelleren Underwriting-Prozess sowie zur Erweiterung des erhältlichen Versicherungsschutzes geführt.

Literatur

- AIG. (2016). M&A-Versicherungen. Haftungsübergang auf den Versicherer. [aig.de. http://www-110.aig.com/2016_067AIGClientEngagementGermany3](http://www-110.aig.com/2016_067AIGClientEngagementGermany3). Zugegriffen am 02.09.2020.
- AIG: Versicherung für Transaktionsrisiken. Einführung. PowerPoint-Präsentation, 2017 file:///C:/Users/T410/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/AIG%20-%20Introduction%20to%20WI%20Insurance%20Presentation%20deutsch%20(April%202017).pdf. Zugegriffen am 18.10.2019.
- CMS European M&A Study (2020). <https://cms.law/en/int/publication/cms-european-m-a-study>. Zugegriffen am 02.09.2020.
- Daghles, M., & Haßler, T. N. (2016). Warranty & Indemnity-Versicherungen im Rahmen von Unternehmenstransaktionen. *Gesellschafts- und Wirtschaftsrecht*, 2016, 455–457.

- Fairhurst, A., & Treagus, M. (2016). W&I not? *CMS Private Equity Watch, Autumn 2016*, 10 f.
- Fingerhuth, J., Fiedler, P., & Froneberg, D. (2016). M&A-Versicherungen als Transaktionsbeschleuniger. PowerPoint-Präsentation, 14. Deutscher Corporate M&A-Kongress vom 14. November 2016. https://convent.de/content/uploads/2016/11/5_MA-Versicherungen_als_Transaktionsbeschleuniger_Pinsent_AIG.pdf. Zugegriffen am 02.09.2020.
- Franz, E. B., & Keune, C. (2013). Warranty and Indemnity Insurance – Die Gewährleistungsversicherung bei Unternehmenskäufen ist auch in Deutschland auf dem Vormarsch. *Versicherungsrecht*, 2013, 1371 ff.
- Froneberg, D., & Dannemann, S. (2017). Beistand für den Break-up. Warranty & Indemnity-Policen als unternehmerischer Sicherheitsfaktor bei Fusionen und Übernahmeprojekten. *Versicherungswirtschaft*, 2017, 21 ff.
- Froneberg, D., Gaul, M., & Kolaric, S. (2017). W&I-Versicherungen als Transaktionsbeschleuniger und erste Schadenserkenntnisse. *M&A Review*, 2017, 216 ff.
- Giessen, P., & Lüttges, M. (2018). Die Bring Down Disclosure in Unternehmenskaufverträgen. *BetriebsBerater*, 2018, 647 ff.
- Giessen, P., & Lüttges, M. (2019). Aktuelle Trends bei W&I-Versicherungen und Abwicklungspraxis bei Schäden. *M&A Review*, 2019, 331 ff.
- Grädler, T., Fritsche, S., & Beilborn, A. (2018). Warranty & Indemnity-Versicherungen bei Unternehmenstransaktionen – Echter Mehrwert oder kurzfristige Modeerscheinung? *Gesellschafts- und Wirtschaftsrecht*, 2018, 464 ff.
- Grossmann, K., & Mönnich, U. (2003). Warranty & Indemnity Insurance, die Versicherbarkeit von Garantierisiken aus Unternehmenskaufverträgen. *NZG*, 2003, 708 f.
- Haberstock, O. (2008). Risikoverteilung im Unternehmenskauf. *P+P Festschrift*, 2008, 29 ff.
- Hasselbach, K., & Reichel, G. (2005). Die Gewährleistungsversicherung als Risikominimierungsmodell in Private-Equity-Transaktionen und sonstigen Unternehmenskäufen. *ZIP*, 2005, 377 ff.
- Hensel C., & Namislo, C. (2018). Die W&I-Versicherung in der M&A-Beratungspraxis. *BetriebsBerater*, 2018, 1475 ff.
- Hermann, H. (2015). Schadensversicherung §39 Kredit- und Kautionsversicherung. In R. M. Beckmann & A. Matusche-Beckmann (Hrsg.), *Versicherungsrechts-Handbuch* (3. Aufl. 2015). München: C.H. Beck.
- Hiort, M. J. (2012). Transaction Insurance zur Überbrückung von (potenziellen) Price Gaps bei M&A-Transaktionen. *Corporate Finance law*, 2012, 127 ff.
- Hoenig, K., & Klingen, S. (2016). Die W&I-Versicherung beim Unternehmenskauf. *NZG*, 2016, 1244 ff.
- Hoger, A., & Baumann, J. (2017). Der M&A-Vertrag bei Abschluss einer W&I-Versicherung. *Neue Zeitschrift für Gesellschaftsrecht*, 2017, 811 ff.
- Hörmann, J. (2008). Die Due Diligence beim Unternehmenskauf. *P+P Festschrift*, 2008, 135 ff.
- Jakobs, M., & Franz, A. (2014). Können W&I-Versicherungen das M&A-Geschäft beleben? *Versicherungsrecht*, 2014, 659 ff.
- Kaufhold, T. (2016). Stapled Insurance bei Private Equity-Transaktionen in Deutschland. *BetriebsBerater*, 2016, 394 ff.
- Klapper, S. (2016). Die Entwicklung von Transaktionsversicherungen (POSI, W&I etc.). *Deutschland, PHi Haftpflicht international – Recht und Versicherung*, 2016, 42 ff.
- Klingenheben, B. (2016). Das Instrument der Warranties & Indemnities-Versicherung zur Absicherung Transaktionsrisiken. *Die VersicherungsPraxis*, 2016, 10 ff.
- Kräzlin, G. P., Otte, S., & Fassbach, B. (2013). Die Gewährleistungsversicherung bei Unternehmenskäufen – neue Entwicklungen und Gestaltungshinweise. *Betriebsberater*, 2013, 2314 ff.

- Kugler, C., & Thiele, C. (2016). Gewährleistungsversicherung – Heilmittel gegen gefährdete Deals? *Investment & Entwicklung*, 2016, 32 f. <https://de.lw.com/thoughtLeadership/Gew%C3%A4hrleistungsversicherung>. Zugegriffen am 02.09.2020.
- Latham & Watkins. (2019). W&I insurance: Exclusions and solutions for private equity. <https://www.latham.london/2019/12/wi-insurance-exclusions-and-solutions-for-private-equity/>. Zugegriffen am 31.08.2020.
- Lips, J. (o. J.). Versicherungen bei M&A-Transaktionen: Effektiver Schutz oder überflüssiges Produkt? cmshs-bloggt.de. <https://www.cmshs-bloggt.de/gesellschaftsrecht/ma/versicherungen-bei-ma-transaktionen-effektiver-schutz-oder-ueberfluessiges-produkt/#>. Zugegriffen am 02.09.2020.
- Metz, F. (2010). Grundzüge der W&I-Insurance beim Unternehmenskauf. *Neue Juristische Wochenschrift*, 2010, 813 ff.
- Oberbracht, D. (2015). Warranty & Indemnity-Versicherungen, Attraktiver Deal-Beschleuniger. *BUJ-Sonderedition M&A Corporate*, 2015, 26 f.
- Rasner, M., Liebau, T., & Knorr, G. (2018). Underwriting 4.0 – Erweiterter Deckungsumfang und Auswirkungen auf den Prozess. *Special M&A Insurance Grundlagen – Praxis – Trends*, Mai 2018, 24 ff.
- Sommer, F., Winter, F., & Knauer, T. (2019). Gewährleistungsversicherungen bei M&A-Transaktionen. *Corporate Finance*, 2019, 118 ff.
- Weitnauer, W. (2016). Der rechtssichere Weg zum Exit: „10 Lehren“ für einen erfolgreichen M&A-Prozess. *Gesellschafts- und Wirtschaftsrecht*, 2016, 413 ff.
- Werlen, S., & Mannsdorfer, T. M. (2013). Versicherung von Transaktionsrisiken. Ein Überblick über die verschiedenen Arten, Verwendungszwecke und Problemstellungen beim Einsatz von M&A Versicherungen. *Gesellschafts- und Kapitalmarktrecht*, 2013, 398 ff.
- Wiegand, D. (2017). Risikomanagement und Streitbeteiligung §84 Gewährleistungsversicherungen (W&I Insurance). In W. Meyer-Sparenberg & C. Jäckle (Hrsg.), *Beck'sches M&A-Handbuch* (1. Aufl. 2017). München: C.H. Beck.

Dr. Carolin van Straelen, LL.M. (Singapore) ist bei AIG Senior Underwriter im Bereich M&A-Versicherungen im deutschsprachigen Raum. Zuvor war sie acht Jahre als Rechtsanwältin bei einer internationalen Großkanzlei in München und Stuttgart sowie einer mittelständischen Kanzlei in München im Bereich Corporate/M&A tätig.

Bernd Dreier, LL.M. (Columbia), ist Rechtsanwalt in München. Zuvor leitete er bei AIG den Bereich M&A-Versicherungen im deutschsprachigen Raum, nachdem er über sechs Jahre als Rechtsanwalt bei internationalen Großkanzleien in Düsseldorf, München und Shanghai im Bereich Corporate/M&A sowie bei einem Investmentfonds tätig war.

Jannik Revers, M.Sc. (Risk and Insurance), Masterstudent der TH Köln (Risk & Insurance). Zuvor Bachelorabschluss im Bereich Versicherungswesen ebenfalls an der TH Köln sowie eine Ausbildung zum Kaufmann für Versicherungen und Finanzen bei der Westfälischen Provinzial. Neben dem Studium wurden praktische Erfahrungen als Werkstudent bei einem Wirtschaftsprüfungsunternehmen, mit Fokus auf Versicherungsunternehmen, gesammelt.



Betriebs- und Produkthaftpflichtversicherung

23

Georg Klinkhammer und Harald Kurtze

Zusammenfassung

Mit der Betriebs- und Produkthaftpflichtversicherung schützen sich Unternehmen gegen Haftpflichtansprüche Dritter wegen Personen-, Sach- und Vermögensschäden. Bei der Ausgestaltung des Versicherungsschutzes für ihre branchentypischen und individuellen Risiken sind Ein- und Ausschlüsse in den AVB, Kriterien für die Wahl der Versicherungssummen sowie Abgrenzungen zu speziellen Haftpflichtdeckungen ebenso zu beachten wie rechtliche, technologische und wirtschaftliche Weiterentwicklungen.

23.1 Einführung

23.1.1 Definitionen

Die Haftpflichtversicherung gehört zur Gruppe der Passivenversicherung. Denn ihre Hauptaufgabe besteht darin, das Vermögen der Versicherten vor den Folgen von Haftpflichtansprüchen Dritter wegen Personen-, Sach- und Vermögensschäden zu schützen.

Im Rahmen der vereinbarten Versicherungsbedingungen leistet der Haftpflichtversicherer Schadenersatz, wenn die Haftpflichtansprüche gegen den Versicherungsnehmer oder Mitversicherte begründet sind (sogenannte Befriedigungsfunktion). Besteht keine

G. Klinkhammer (✉)

Gesamtverband der versicherungsnehmenden Wirtschaft e. V., Bonn, Deutschland

E-Mail: georg-klinkhammer@t-online.de

H. Kurtze

TH Köln, Institut für Versicherungswesen, Köln, Deutschland

E-Mail: haraldkurtze@gmail.com

Schadenersatzpflicht, weist der Versicherer die zu Unrecht erhobenen Ansprüche auf seine Kosten zurück (sogenannte Abwehrfunktion).

Versicherungsnehmer einer Betriebs- und Produkthaftpflichtversicherung sind vor allem Industrie-, Gewerbe- Handels- und Handwerksbetriebe sowie sonstige Dienstleister.

Der Umfang der Deckung erstreckt sich insbesondere auf Schadenfälle,

- die von der Betriebsstätte ausgehen, also von dem Betriebsgrundstück, den Geschäftsräumen und den verwendeten Produktionsanlagen;
- die durch im Unternehmen tätige Personen verursacht werden;
- die bei Produktions- und Handelsbetrieben durch veräußerte Produkte entstehen.

Ansprüche Dritter können aus einer verschuldensabhängigen (zum Beispiel §§ 823 ff BGB) oder einer verschuldensunabhängigen Haftung bzw. Gefährdungshaftung (zum Beispiel Produkthaftungsgesetz) des Versicherungsnehmers resultieren.

Ein besonderes Augenmerk liegt auf der industriellen Massenproduktion als potenziell Multiplikator von Schadenquellen. Die Haftpflichtversicherung bietet hier einen elementaren Beitrag zur Existenzsicherung von Unternehmen, die vor allem im Großschadensfall unentbehrlich ist.

Die Produkthaftpflichtversicherung (ProdHV) ist keine eigenständige Versicherung, sondern sie wird (je nach Bedarf des Unternehmens) mit der Betriebshaftpflichtversicherung (BHV) kombiniert. Traditionell wird zwischen der konventionellen ProdHV und der erweiterten ProdHV unterschieden. Die konventionelle PHV bezieht sich auf die Versicherung von Personen- und Sachschäden einschließlich der daraus resultierenden Folgeschäden durch mangelhafte Produkte, während die erweiterte ProdHV darüber hinaus bestimmte reine Vermögensschäden (zum Beispiel Aus- und Einbaukosten) durch mangelhafte Produkte erfasst. Die konkrete Zuordnung der Deckungsmodule wird in den jeweils vereinbarten Versicherungsbedingungen geregelt, zum Beispiel in den AVB BHV durch A1-7.26, A3-1.1 sowie A3-7.

23.1.2 Rechtsgrundlagen

Die gesetzlichen Grundlagen der Betriebs- und Produkthaftpflichtversicherung sind vorwiegend im Bürgerlichen Gesetzbuch (BGB) sowie im Versicherungsvertragsgesetz (VVG) verankert.

Die vertraglichen Grundlagen bilden insbesondere die „Allgemeine Versicherungsbedingungen für die Haftpflichtversicherung“ (AHB), die „Allgemeine Versicherungsbedingungen für die Betriebs- und Berufshaftpflichtversicherung“ (AVB BHV) sowie die „Besondere Bedingungen und Risikobeschreibungen für die Produkthaftpflichtversicherung von Industrie- und Handelsbetrieben“, das sogenannte Produkthaftpflicht-Modell (ProdHM); hierbei handelt es sich jeweils um Musterbedingungen des Gesamtverbandes der Deutschen Versicherungswirtschaft e. V. (GDV).

Diverse Zusatzbedingungen sowie Besondere Bedingungen und Risikobeschreibungen (BBR) enthalten weitere spezielle Regelungen zum Versicherungsschutz. Die AVB dienen hier als Allgemeine Geschäftsbedingungen (AGB), auf welche die weiteren Regeln der Betriebshaftpflichtversicherung aufbauen.

23.1.3 Abgrenzung

Abzugrenzen ist die klassische BHV wie auch eine integrierte ProdHV von anderen Haftpflichtversicherungen, auf welche entweder der Deckungszuschnitt der BHV und der ProdHV nicht passt oder deren Anwendungsbereich dort ausdrücklich ausgeschlossen wird (zum Beispiel A3-7.7.3 AVB BHV-Rückrufkosten).

23.1.3.1 Privathaftpflichtversicherung

Die Privathaftpflichtversicherung schützt Versicherte bei Haftpflichtansprüchen wegen Schäden, die aus privaten Tätigkeiten resultieren.

23.1.3.2 Berufshaftpflichtversicherung

Eine Berufshaftpflichtversicherung bietet Versicherungsschutz, wenn Versicherte als Freiberufler (Rechtsanwalt, Steuerberater, Wirtschaftsprüfer etc.) wegen Vermögensschäden im Zusammenhang mit einer beruflichen Tätigkeit in Haftung genommen werden.

23.1.3.3 Umwelthaftpflichtversicherung

Die Umwelthaftpflichtversicherung deckt zivilrechtliche Ansprüche gegen Versicherte wegen Schäden Dritter, die durch Umwelteinwirkungen über einen sogenannten Umweltpfad (Boden, Luft, Wasser) entstanden sind.

23.1.3.4 Umweltschadensversicherung

Die Umweltschadensversicherung tritt ein, wenn Versicherte öffentlich-rechtlich (Umweltschadensgesetz) wegen Kosten zum Beispiel für die Sanierung von Schäden an geschützten Arten, Gewässern oder natürlichen Lebensräumen belangt werden.

23.1.3.5 Rückrufkostenhaftpflichtversicherung

Die (Allgemeine oder die Kfz-)Rückrufkosten-Haftpflichtversicherung übernimmt bestimmte Vermögensschäden bzw. Kosten (zum Beispiel Benachrichtigungs- und Sortierkosten) aus Rückrufaktionen, die zwecks Abwendung von Personenschäden durchgeführt worden sind. Es kann sich sowohl um eigene Rückrufe des Versicherungsnehmers, als auch um Fremdrückrufe handeln, die entsprechende Regressforderungen gegenüber dem Versicherungsnehmer als Zulieferer zur Folge haben.

23.2 Bedeutung für die Unternehmenspraxis

23.2.1 Beispiele für Risiko- und Haftungsszenarien

23.2.1.1 Leitungsschäden

Bei vielen Unternehmen aus speziellen Branchen (zum Beispiel Versorgungsunternehmen und Bauunternehmen) zählen Leitungsschäden zu den wichtigsten Haftungsrisiken. Sie bergen ein hohes Schadenpotenzial. Mit Blick auf die wachsende Bedeutung der Errichtung neuer und der Sanierung bestehender Versorgungseinrichtungen mit unterschiedlichen Gewerken dürfte der Stellenwert dieser Risiken bei vielen Versicherungsnehmern noch wachsen (vgl. Bauer 2019, S. 3).

Deckungsrechtlich sind Leitungsschäden ein Unterfall von Schäden durch Bearbeitung fremder Sachen (Tätigkeitsschäden). Gemäß A1-6.7.2 AVB BHV ist die gesetzliche Haftpflicht des Versicherungsnehmers wegen Tätigkeitsschäden an Erdleitungen (Kabel, unterirdische Kanäle, Wasserleitungen, Gasrohre und andere Leitungen) sowie Frei- oder Oberleitungen mitversichert.

Neben den direkten Sachschäden können bei Leitungsschäden insbesondere auch erhebliche Vermögensfolgeschäden auftreten. Versicherungsnehmer mit einschlägigen Risikoprofilen müssen deshalb insbesondere auf eine angemessene Versicherungssumme für Leitungsschäden achten.

23.2.1.2 Produkt-Serienschäden

Der Massenabsatz von Erzeugnissen erhöht die Gefahr von Serienschäden, die immense Kosten verursachen können. Hat zum Beispiel ein Armaturenhersteller 5000 Armaturen ausgeliefert, die bei diversen Kunden weltweit eingebaut worden sind, und müssen die Armaturen wegen Spannungsrissen ausgetauscht werden, können sich die Austauschkosten in Höhe von mehreren hunderttausend Euro bewegen (vgl. Seiring et al. 2016, S. 67).

Die Haftpflichtversicherer sehen für die deckungsrechtliche Behandlung von Serienschäden unterschiedliche Serienschadenklauseln vor. Gemäß Ziff. 8.3 ProdHM werden Serienschäden deckungsrechtlich wie folgt behandelt:

„Mehrere während der Wirksamkeit des Vertrages eintretende Versicherungsfälle aus der gleichen Ursache, zum Beispiel aus dem gleichen Konstruktions-, Produktions- oder Instruktionsfehler, es sei denn, es besteht zwischen den mehreren gleichen Ursachen kein innerer Zusammenhang, oder aus Lieferungen solcher Erzeugnisse, die mit den gleichen Mängeln behaftet sind, gelten unabhängig von ihrem tatsächlichen Eintritt als in dem Zeitpunkt eingetreten, in dem der erste dieser Versicherungsfälle eingetreten ist.“

Hinsichtlich der „gleichen Ursache“ werden hier beispielhaft Fehlerquellen genannt (vgl. zum Ganzen Littbarski 2014, S. 402; vgl. Nickel und Nickel-Fiedler 2015, S. 169):

- Konstruktionsfehler ist ein Fehler, der regelmäßig die gesamte Serie erfasst und im Stadium der Produktplanung verursacht wird.

- Produktionsfehler ist ein Fehler, der die gesamte Serie oder nur einen Teil der Serie erfasst und dadurch die fehlerhafte Planung, Durchführung oder Kontrolle der Produktionsabläufe verursacht.
- Instruktionsfehler ist der Mangel eines Produktes, der darin besteht, dass eine fehlerhafte Anwendungsberatung bei im Übrigen fehlerloser oder fehlerhafter Sache die konkrete Gefahr von Schäden bei der Anwendung der Sache mit sich bringt.
- Eine Ursachenserie ist dann nicht anzunehmen, wenn zwischen den Ursachen kein innerer Zusammenhang besteht.

In Industrieverversicherungsverträgen können auch anders lautende Serienschadenklauseln vereinbart werden. Je nach Formulierung einer Serienschadenklausel ergeben sich unterschiedliche Konsequenzen, etwa für die Gestaltung der Versicherungssummen und Selbstbeteiligungen sowie für den Fall eines Versichererwechsels.

23.2.2 Reichweite und Grenzen der Deckung

Die Reichweite des jeweiligen Versicherungsschutzes wird zum einen durch die vereinbarten Versicherungssummen und zum anderen durch die in den Versicherungsbedingungen aufgeführten Ausschlusstatbestände begrenzt.

23.2.2.1 Versicherungssummen

Unterschiedliche Konstellationen zur Festlegung der Versicherungssummen sind zum Beispiel in A 1-5 der AVB BHV und in Ziff. 9.1 ProdHM aufgeführt, wobei dort explizit eine mögliche Differenzierung nach Personenschäden einerseits sowie Sach- und Vermögensschäden andererseits angesprochen wird.

Faktoren, die für die Bestimmung der Versicherungssummen herangezogen werden können, sind zum Beispiel:

- welches Produkt zu welchem Einsatzzweck hergestellt wird,
- ob die Fertigung des Produkts ausschließlich im In- oder auch Ausland erfolgt,
- welche und wie viele Personen am Produktionsprozess beteiligt sind,
- welche Schäden (Personen-, Sach- und/oder Vermögensschäden) vorrangig möglich sind,
- ob das Produkt nur im Inland oder auch im Ausland vertrieben werden soll und
- wie die Haftungsgefahren aufgrund der durch Gesetz oder Rechtsprechung geprägten jeweiligen Rechtslage einzuschätzen sind.

Es ist zu beobachten, dass mittelständische Unternehmen ihre Produkthaftpflichtrisiken nicht selten unterschätzen. Das kann dazu führen, dass es vor allem bezüglich der (erweiterten) Produkthaftpflichtversicherung (Stichwort: reine Vermögensschäden) an der Vereinbarung einer angemessenen Versicherungssumme mangelt. Fachkundige Begleitung

durch Makler, Rechtsanwälte oder andere Berater, aber auch durch den Haftpflichtversicherer, ist an dieser Stelle nützlich und empfehlenswert.

In diesem Zusammenhang ist auch die Jahresmaximierung der Versicherungssummen von Bedeutung. Die Begrenzung der Leistungspflicht des Versicherers für alle Versicherungsfälle eines Versicherungsjahres in Gestalt einer Höchstversatzleistung entspricht der üblichen Praxis bei allen Arten der Haftpflichtversicherung. Aus der Sicht des Versicherers soll damit sichergestellt werden, dass das übernommene Risiko überschaubar, begrenzbar und damit kalkulierbar ist (vgl. Nickel und Nickel-Fiedler 2015, S. 423). Dem Versicherungsnehmer wird durch die Jahresmaximierung verdeutlicht, dass der Versicherungsschutz nicht im unbegrenzten Maße pro Versicherungsjahr zur Verfügung steht und dass er eventuelle Schäden, die über das Jahreshöchstlimit hinausgehen, selbst tragen muss (vgl. Littbarski 2014, S. 423).

23.2.2.2 Ausschlusstatbestände

Sowohl in der BHV als auch in der ProdHV gibt es eine Reihe von Ausschlüssen und Risikobegrenzungen, die es bei der Ausgestaltung des Versicherungsschutzes zu beachten gilt. Zum Teil werden diese Deckungseinschränkungen in der Praxis als nicht verhandelbar betrachtet, zum Teil besteht Verhandlungsspielraum und zum Teil können spezielle (zusätzliche) Deckungen für die ausgeschlossenen Risikobereiche vereinbart werden.

Ausschlussbestimmungen sind vor allem in Ziff. 1.2 und Ziff. 7 AHB, in A1-7. AVB BHV und in Ziff. 6 ProdHM sowie in sonstigen Bedingungen zu den jeweiligen Versicherungen zu finden.

Neben marktüblichen Ausschlüssen, wie zum Beispiel für vorsätzlich herbeigeführte oder durch Kriegsereignisse entstandene Schäden, werden in den AHB BHV weitere Ausschlüsse benannt:

Gemäß Ziff. A1-7.2 sind Versicherungsansprüche aller Personen, die den Schaden dadurch verursachen, dass sie in Kenntnis von deren Mangelhaftigkeit oder Schädlichkeit Arbeiten oder sonstige Leistungen erbringen, ausgeschlossen. Als Hintergrund dieses Ausschlusses sieht man zum Beispiel das Spannungsfeld, in dem sich Unternehmen bewegen, deren Kunden zunehmend eine low price-Erwartungshaltung kommunizieren. Denn dieser Umstand könnte dazu führen, dass Unternehmen Produkte veräußern, von denen sie wissen, dass sie nicht frei von Mängeln sind. In diesen Fällen wird zwar kein Schaden vorsätzlich herbeigeführt, mitunter jedoch billigend in Kauf genommen (vgl. Nickel und Nickel-Fiedler 2015, S. 191).

Zu beachten ist auch der Ausschluss in Ziff. A1-7.3 für Ansprüche der Versicherten untereinander. Dieser Ausschluss betrifft Ansprüche zwischen mehreren Versicherungsnehmern desselben Versicherungsvertrags. Bei Bedarf kann in der Praxis eine Abänderung dieses Ausschlusses verhandelt und umgesetzt werden.

Laut Ziff. A1-7.7 sind Haftpflichtansprüche, die auf Asbest sowie asbesthaltige Substanzen oder Erzeugnisse zurückzuführen sind, ausgeschlossen.

Ziff. A1-7.8 schließt Ansprüche wegen Schäden, die zurückzuführen sind auf gentechnische Arbeiten, gentechnisch veränderte Organismen (GVO) sowie Erzeugnisse, die Bestandteile aus GVO enthalten, aus GVO oder mithilfe von GVO hergestellt wurden, ebenfalls aus. In Industriever sicherungspolicen werden darüber hinaus oftmals weitere „stoffbezogene“ Ausschlüsse aufgenommen (zum Beispiel für chlorierte Kohlenwasserstoffe).

Gemäß Ziff. A1-7.19 sind Ansprüche auf Entschädigung mit Strafcharakter, insbesondere punitive oder exemplary damages, nicht gedeckt. Damit wird der vor allem in den USA verhängte Strafschadenersatz von der Deckung ausgeschlossen, der über den tatsächlich entstandenen Schaden hinausgeht. Für hiesige Versicherer und Versicherungsnehmer ist das von Bedeutung, weil die Haftpflichtpolicen von Industrieunternehmen grundsätzlich auch Auslandsschäden (weltweit) einschließen.

Schließlich enthält Ziff. A1-7.20 einen Ausschluss für Ansprüche nach Art. 1792 ff. und den damit im Zusammenhang stehenden Regressansprüchen nach Art. 1147 des französischen Code Civil oder gleichartiger Bestimmungen anderer Länder. Betroffen sind hiervon vorrangig Unternehmen der Bauwirtschaft, die bei Aktivitäten in Frankreich etc. einer Versicherungspflicht nach dortigen Usancen unterliegen.

23.3 Auslegung von Bedingungen und Rechtsprechung

23.3.1 Abgrenzung Haftpflicht-/Erfüllungsanspruch

Das OLG Dresden hat sich mit Urteil vom 23.10.2013 – 7 U 548/13 mit einer der umstrittensten Fragestellungen in der industriellen und gewerblichen Haftpflichtversicherung befasst, nämlich mit der Unterscheidung zwischen einem nicht gedecktem Erfüllungsschaden (§ 4 Abs. 1 Nr. 6 AHB alte Fassung bzw. Ziff. 1.2 AHB neue Fassung) und einem gedeckten Folgeschaden.

Dem Urteil lag folgender Sachverhalt zugrunde:

Der Versicherungsnehmer hatte sich zur Lieferung, Montage und Inbetriebnahme der Gewerke Heizung, Lüftung und Sanitär verpflichtet. Die Gewerke Abwasser-, Wasser und Gasanlagen waren mit dem Gewerk Wärmeversorgungsanlagen in einem Hauptauftrag zusammengefasst. In einem Leistungsverzeichnis waren die Gesamtpreise zusammengerechnet worden. Sonstige Zusammenhänge zwischen den Gewerken bestanden nicht. Insbesondere wurden keine Leistungsteile, wie etwa die Baustelleneinrichtung, für beide Gewerke gemeinsam angeboten. Die Gewerke wurden auch räumlich und zeitlich deutlich voneinander getrennt erbracht.

Es kam zu einem Wasserschaden, der sich im gesamten Gebäudeteil auswirkte. Deshalb musste sowohl die Fußbodenheizung als auch die Dämmung zwecks Schadenbehebung entfernt werden. Im Hinblick darauf, dass die Erneuerung der Fußbodenheizung lange vor dem Eintritt des Wasserschadens abgenommen worden war, rechnete das OLG

den Schaden nicht dem vom Versicherungsschutz ausgeschlossenen Erfüllungsbereich zu. Zur Begründung führte das Gericht an, es habe sich nicht um einen einheitlichen Leistungsgegenstand gehandelt. Vielmehr sei der Schaden am bereits abgeschlossenen Werkleistungsteil Fußbodenheizung als Folgeschaden zu betrachten. Diese Argumentation gelte sowohl im Hinblick auf den Erfüllungsausschluss gemäß § 4 Abs. 1 Nr. 6 AHB alte Fassung bzw. Ziff. 1.2 AHB neue Fassung als auch im Hinblick auf die Herstellungsklausel in § 4 Abs. 2 Nr. 5 AHB alte Fassung bzw. Ziff. 7.8 AHB neue Fassung

Somit kann festgehalten werden, dass selbst bei Gewerken, die aufgrund eines einheitlichen Werkvertrages errichtetet worden sind, unter bestimmten Umständen von mehreren Leistungsgegenständen ausgegangen werden kann. In diesen Fällen ist ein bereits abgeschlossener, abgenommener und durch Arbeiten des Versicherungsnehmers beschädigter Leistungsteil nicht als Erfüllungsschaden vom Haftpflichtversicherungsschutz ausgenommen.

Das OLG Köln hat mit Beschluss vom 31.01.2019 – 9 U 72/18 entschieden, dass Ansprüche wegen Schäden an zu bearbeitenden Sachen des Auftraggebers des Versicherungsnehmers (vom Auftraggeber „bereitgestellte Sachen“) dem Erfüllungsschadenausschluss unterfallen und in der Betriebshaftpflichtversicherung nicht gedeckt sind.

Die Klägerin, die als Gläubigerin der zwischenzeitlich insolventen Versicherungsnehmerin Ansprüche gegen die Beklagte als Haftpflichtversicherer geltend machte, hatte die Versicherungsnehmerin beauftragt, von ihr bereit gestellte Fassadenplatten zu lackieren. Die Versicherungsnehmerin nahm diese Lackierung vor und stellte die Fassadenplatten zur Abholung bereit. Die Klägerin holte die Fassadenplatten ab und musste an der Baustelle feststellen, dass die Platten zusammenklebten. Beim Trennen der Platten lösten sich die Farboberflächen. Die Klägerin machte Ansprüche aufgrund der irreparabel beschädigten Platten geltend. Über die Ansprüche erwirkte sie vor Eröffnung des Insolvenzverfahrens einen Vollstreckungsbescheid gegen die Versicherungsnehmerin. Die titulierte Forderung machte die Klägerin nunmehr gegen den Haftpflichtversicherer geltend.

In der Haftpflichtpolice der Beklagten war unter anderem folgende Regelung vereinbart: „Eingeslossen ist die gesetzliche Haftpflicht aus Schäden, die an fremden Sachen durch eine gewerbliche oder berufliche Tätigkeit an oder mit diesen Sachen entstanden sind und alle sich daraus ergebenden Vermögensschäden, wenn diese Schäden durch eine gewerbliche oder berufliche Tätigkeit des Versicherungsnehmers entstanden sind ... Die Regelungen von Nr. 7 a (Schäden an hergestellten oder gelieferten Arbeiten oder Sachen) und § 39 Nr. 1 (Erfüllungsansprüche) bleiben bestehen. Ausgeschlossen bleiben Haftpflichtansprüche wegen Tätigkeitsschäden an Sachen, die sich beim Versicherungsnehmer zur Lohnbe- und/oder -verarbeitung oder zu sonstigen Zwecken befinden, befunden haben oder die vom Versicherungsnehmer übernommen wurden. Dieser Ausschluss gilt jedoch nur für solche Schäden, die bei dem unmittelbaren Bearbeitungsvorgang entstanden sind. Zu unmittelbaren Bearbeitungsvorgängen zählen nicht zum Beispiel vor- oder nachgelagerte Verpackungstätigkeiten, Transporttätigkeiten oder Lagerung der Sachen. In teilweiser Abänderung besteht jedoch auch für Schäden, die beim unmittelbaren Bearbeitungsvorgang entstanden sind, Versicherungsschutz.“

Nach Auffassung des OLG Köln werden durch die Tätigkeitsschadenklausel keine, auch nicht teilweise, Erfüllungsansprüche gedeckt. Zumindest bei Bedingungen, die in einem gesonderten Absatz auf die Geltung der Erfüllungsklausel hinweisen, welche die Tätigkeitsschadenklausel nicht vom Grundsatz des unversicherten Unternehmer- und Erfüllungsrisiko ab.

Die Bereitstellung und Durchtrocknung von Fassadenplatten im Rahmen einer Lackierung seien als Bestandteile einer ordnungsgemäßen Vertragserfüllung einzuordnen, weshalb Ansprüche aufgrund eines Zusammenklebens der Platten nach dem Lackieren und damit vorliegender irreparabler Beschädigung allein dem nicht versicherten Erfüllungsinteresse zuzuordnen seien.

23.3.2 Reichweite eines subjektiven Ausschlusses

Das OLG Koblenz hat mit Beschluss vom 17.03.2014 – 10 U 1170/13 die Reichweite eines Deckungsausschlusses für bewusst pflichtwidriges Verhalten in der Betriebshaftpflichtversicherung bewertet.

Nach Auffassung des OLG ist der Haftpflichtversicherer dem Versicherungsnehmer gegenüber nicht eintrittspflichtig, wenn ein Drittschaden dadurch herbeigeführt worden ist, dass ein beim Versicherungsnehmer angestellter Kranführer Lasten bewegt hat, ohne freie Sicht auf das Arbeitsfeld zu haben.

Diese Entscheidung kann man kritisch sehen: Es ist zwar richtig, dass sich ein Unternehmen das Verhalten und Verschulden eines Mitarbeiters haftungsrechtlich nach § 278 BGB zurechnen lassen muss. Auch trifft es zu, dass im Rahmen der Betriebshaftpflichtversicherung versicherte Mitarbeiter gemäß § 47 Abs. 1 VVG ihren persönlichen Versicherungsschutz verlieren, wenn sie den Haftpflichtschaden bewusst pflichtwidrig herbeigeführt haben. In versicherungsrechtlicher Hinsicht erfolgt eine Zurechnung des Verhaltens eines Mitarbeiters zu Lasten des versicherten Unternehmens aber nur dann, wenn der betreffende Mitarbeiter Repräsentant des Unternehmens gewesen ist.

Bei Heranziehung der Maßstäbe der Rechtsprechung des BGH an die Voraussetzungen einer Repräsentantenstellung (Befugnis, für den Versicherungsnehmer selbstständig in nicht ganz unbedeutendem Umfang zu handeln) konnte der Kranführer, der hier weder Risiko- noch Vertragsverwalter des Unternehmens war, nicht als Repräsentant betrachtet werden. Deshalb hätte das Unternehmen seinen Haftpflichtversicherungsschutz im konkreten Fall behalten müssen, falls ihm selbst keine bewusste Pflichtwidrigkeit vorzuwerfen war (vgl. Schimikowski 2015, S. 232).

Es bleibt anzumerken, dass in Versicherungspolicen zu Gunsten des Deckungsschutzes des Versicherungsnehmers ausdrücklich eine (enge) Definition des Repräsentanten vereinbart werden kann (nur „die gesetzlichen Vertreter“).

23.3.3 Auslegung eines individuellen Ausschlusses

Wie ein individueller Leistungsausschluss durch Gerichte ausgelegt werden kann, beleuchtet ein Urteil des OLG Düsseldorf vom 23.03.2018 – 4U 60/17. In dem Fall ging es um Schäden an zu kommissionierender Ware.

Der Versicherungsnehmer machte Ansprüche gegen den Versicherer aus einer Betriebshaftpflichtversicherung geltend. Versichertes Risiko war unter anderem die gesetzliche Haftpflicht des Versicherungsnehmers als Unternehmerin des versicherten Betriebes, der im Versicherungsschein als „Sonstiger Großhandel (Endprodukte) – Kommissionierung von Tiefkühlkost auf fremdem Grundstück“ bezeichnet war.

In einem externen Logistikzentrum betrieb der Versicherungsnehmer ein Tiefkühllager. In dem Lager befand sich von einem Dritten im eigenen Namen und für eigene Rechnung gekaufte Ware, die im eigenen Namen für eigene Rechnung verkauft werden sollte.

Im Versicherungsschein lautete ein Passus unter der Überschrift „Individuelle Vereinbarungen“: „Jegliche Ansprüche aus Schäden an den zu kommissionierenden Waren und Kartonagen bzw. Verpackungsmaterialien sowie daraus resultierende Folgeschäden sind nicht versichert.“

Der Versicherungsnehmer trug vor, dass einer seiner Mitarbeiter mit einem Gabelstapler unbemerkt die Sprinkleranlage in dem Tiefkühllager ausgelöst habe. Das Löschmittel sei auf die Ware (sowohl die Lagerware im Hochregal als auch die bereits kommissionierte Ware auf den Paletten) getropft und habe diese unbrauchbar gemacht. Ferner seien Schäden an der Sprinkleranlage, den Deckenplatten etc. entstanden.

Der Versicherer war der Meinung, er müsse den Schaden, für den der Versicherungsnehmer haftete, nur zum Teil ausgleichen. Nicht zu übernehmen seien die „Kosten im Zusammenhang mit der Kommissionsware“.

Das OLG Düsseldorf urteilte zu Gunsten des Versicherungsnehmers. Die als individuelle Vereinbarung bezeichnete Leistungsausschlussklausel für Schäden an Kommissionsware war nach Auffassung des OLG nicht einschlägig. Das OLG verweist auf die ständige Rechtsprechung des BGH, wonach der durchschnittliche Versicherungsnehmer nicht damit zu rechnen braucht, dass er Lücken im Versicherungsschutz hat, ohne dass die Klausel ihm dies hinreichend verdeutlicht.

Dieser Grundsatz ist laut OLG auch dann heranzuziehen, wenn eine Klausel nicht für eine Vielzahl von Verträgen verwendet werden soll und demnach nicht als Allgemeine Bedingung anzusehen ist, aber nichtsdestotrotz nicht zwischen den Parteien im Rahmen gemeinsamer Verhandlungen ausgehandelt, sondern einseitig vom Versicherer insbesondere hinsichtlich des Wortlauts vorgegeben wurde. So lag der Fall hier, da es unstreitig kein besonderes Gespräch über die Ausschlussklausel zwischen den Parteien gegeben hatte.

Es bestand kein Streit darüber, dass tatsächlich sämtliche Waren, die sich im Tiefkühllager befanden, zu einem in der Zukunft liegenden Zeitpunkt zu kommissionieren gewesen wären, falls der Schadensfall nicht eingetreten wäre. Dies genügte laut OLG allerdings

nicht, um sämtliche Waren im Lager, die irgendwann zu einem völlig ungewissen Zeitpunkt zu kommissionieren wären, vom Versicherungsschutz auszuschließen.

Vom Wortlaut gedeckt sei vielmehr auch ein Verständnis, wonach lediglich Schäden an solchen Waren ausgeschlossen sein sollten, die sich in einem konkreten Kommissionierungsvorgang befanden, die also gegenwärtig zu kommissionieren waren und nicht erst zu einem unbestimmten und ungewissen Zeitpunkt in der nahen oder sogar fernen Zukunft. Aufgrund dessen war der Wortlaut der Klausel letztlich offen und stand einer eingeschränkten Auslegung jedenfalls nicht entgegen.

Für ein engeres Verständnis der zu kommissionierenden Waren sprach nach Meinung des OLG schließlich auch der Sinn und Zweck der Leistungsausschlussklausel. Erst durch den Vorgang des Kommissionierens sei die konkret davon betroffene Ware einem deutlich erhöhten Risiko ausgesetzt, da sie aus dem Hochregal entnommen, transportiert und dann zur Kommission zusammengestellt werde.

23.4 Spezielle Klauseln und Gestaltungsmöglichkeiten

23.4.1 Vertragliche Haftungsregelungen

Gemäß Ziff. A1-3.3 AVB BHV besteht kein Versicherungsschutz für Ansprüche, soweit sie aufgrund einer vertraglichen Vereinbarung oder Zusage über den Umfang der gesetzlichen Haftpflicht des Versicherungsnehmers hinausgehen.

Das Thema der Vertragshaftung ist von erheblicher praktischer Bedeutung für Versicherungsnehmer, da diese gegenüber ihren Geschäftspartnern oftmals vertragliche Haftungszusagen erklären müssen, die den gesetzlich definierten Haftungsrahmen überschreiten.

So verpflichten Abnehmer ihre Lieferanten beispielsweise im Rahmen von Qualitätssicherungsvereinbarungen häufig, sie von ihren Prüf- und Rügepflichten gemäß § 377 HGB zu entbinden, und viele Versicherungsnehmer vereinbaren mit ihren Kunden längere Verjährungsfristen, als gesetzlich vorgesehen. Die Verjährungsfristen betragen gemäß § 438 BGB bei Kaufverträgen zwei Jahre und bei Verträgen, die Bauwerke zum Gegenstand haben, fünf Jahre.

Grundsätzlich ist es möglich, mit dem Haftpflichtversicherer durch eine spezielle „Klausel zu kaufmännischen Prüf- und Rügepflichten“ und eine „Klausel zur Verlängerung der Gewährleistungspflicht“ zu regeln, dass der Versicherer sich in den genannten bzw. in konkret definierten Fällen nicht auf den Ausschluss in Ziff. A1-3.3 berufen wird (vgl. Seiring et al. 2016, S. 72).

23.4.2 Erprobungsklausel

Unternehmen entwickeln ihre Produkte regelmäßig weiter. In diesem Zusammenhang ist die sogenannte Erprobungsklausel beachten. Denn gemäß Ziff. 6.2.5 S. 1 ProdHM sind Ansprüche aus Sach- und Vermögensschäden (nicht also Personenschäden) durch Erzeugnisse, deren Verwendung oder Wirkung im Hinblick auf den konkreten Verwendungszweck nicht nach dem Stand der Technik oder in sonstiger Weise ausreichend erprobt waren, vom Versicherungsschutz ausgeschlossen.

Mit der Erprobungsklausel wollen Versicherer verhindern, dass sie zur Nachfinanzierung herangezogen werden, wenn ein Versicherungsnehmer zum Beispiel aus Kosten- oder Wettbewerbsgründen ein Produkt auf den Markt bringt, ohne es vorher ausreichend erprobt zu haben (vgl. Späte und Schimkowski 2015, S. 938; vgl. Czeremuga 2017, S. 40).

Sachlich erstreckt sich dieser Ausschlusstatbestand auf sämtliche in Verkehr gebrachte Erzeugnisse und somit nicht nur auf Neuentwicklungen, also auch auf weiterentwickelte oder geänderte Produkte, die weiterhin in den Verkehr gebracht werden. In zeitlicher Hinsicht kommt es für die Erprobung auf den Zeitpunkt des Inverkehrbringens an (vgl. Loschelders et al. Ziff. 6 ProdHaftPflV Rn. 306).

Der Erprobungsausschluss findet nur Anwendung, wenn zwischen den Schäden an den Sachen und den hergestellten oder gelieferten Erzeugnissen ein Funktionszusammenhang besteht oder diese deren bestimmungsgemäßer Einwirkung unterliegen. Wird zum Beispiel bei der Verwendung einer nicht ausreichend erprobten Turbine durch den Abnehmer ein angeschlossener Generator beschädigt, greift die Erprobungsklausel, da zwischen dem Generator und der Turbine ein Funktionszusammenhang besteht. Hingegen wären etwaige Schäden an Wänden oder Fenstern in der Werkshalle des Kunden gedeckt (vgl. Thürmann und Kettler 2009, S. 291 f.).

Der zentrale Maßstab dafür, ob ein Erzeugnis ausreichend erprobt wurde, ist der „Stand der Technik“. Hierbei handelt es sich um einen unbestimmten Begriff, der je nach Lage des Einzelfalles zu werten ist. Bei der Beurteilung ist auch der Unterschied zwischen den Begriffen „Stand der Technik“ und „Stand der Wissenschaft und Technik“ zu beachten. So werden bei letzterem unter anderem fortschrittliche Verfahren berücksichtigt, welche auch experimenteller Natur sein können. Zur Durchführung derartiger Verfahren ist der Versicherungsnehmer nicht verpflichtet. Auf der anderen Seite kann der Versicherungsnehmer sich nicht auf die Einhaltung des Stands der Technik berufen, sofern er einen Standard verwendet, der nicht der aktuellen technischen Entwicklung entspricht (vgl. Prölls et al. 2018, Ziff. 6 ProdHaftPfl Rn. 10).

Der Versicherer hat das Vorliegen der Voraussetzungen der Ausschluskklausel zu beweisen, was mit Schwierigkeiten verbunden sein kann. Denn es müssen negative Tatsachen aus der betrieblichen Sphäre des Versicherungsnehmers nachgewiesen werden (Späte und Schimkowski 2015, S. 941), wobei allerdings von der Rechtsprechung entwickelte Grundsätze der Beweiserleichterung zu Gunsten des Versicherers eingreifen können.

In der Praxis lässt sich eine Tendenz erkennen, nach der Versicherer bei komplexen Schäden zur erweiterten Produkthaftpflichtversicherung häufiger die Erprobungsklausel

heranziehen, um den Versicherungsschutz in Zweifel zu ziehen. Als Argument wird dann etwa vorgebracht, dass sich die Produktzyklen und damit die Entwicklungszyklen beim Versicherungsnehmer verkürzt hätten und für eine ausreichende Erprobung zu wenige Mittel einkalkuliert worden seien, so dass die Erprobung sozusagen im Feld stattfinde.

Versicherungsnehmer müssen deshalb darauf achten, dass sie durch geeignete Nachweise, insbesondere durch eine möglichst ausführliche und umfangreiche Dokumentation des Entwicklungs- und Erprobungsprozesses, solche Argumente des Versicherers entkräften können.

Soweit zur Erprobungsklausel veröffentlichten Gerichtsurteile ergangen sind, wurden diese bislang zu Gunsten des Versicherers entschieden. Deshalb sollten die Versicherungsnehmer versuchen, die Erprobungsklausel durch vertragliche Modifikationen abzumildern, zum Beispiel durch eine Präzisierung der Anforderungen an eine ausreichende Erprobung oder durch Ausgestaltung der Klausel als Obliegenheit (vgl. Czeremuga 2017, S. 42).

23.4.3 Produktausfalldeckung

Die Produktausfalldeckung ist eine spezielle Deckungserweiterung, die von wenigen Haftpflichtversicherern für bestimmte Branchen der Investitionsgüterindustrie (zum Beispiel Fahrzeugbau, Maschinenbau oder Elektrotechnik) entwickelt wurde und seit wenigen Jahren angeboten wird. Es geht um eine Einbeziehung von reinen Vermögensschäden durch Produkte, die über die Inhalte einer klassischen erweiterten Produkthaftpflichtversicherung mit ihren abschließend genannten Vermögensschadentatbeständen (zum Beispiel Aus- und Einbaukosten) hinausgeht. Mitunter wird diese Deckungserweiterung auch Nutzungsausfalldeckung oder offene Produkt-Vermögensschadendeckung genannt (vgl. Klinkhammer 2015, S. 3).

Konkret geht es um die Versicherung von Ansprüchen Dritter, zum Beispiel wegen Betriebsunterbrechung, Nutzungsausfalls oder sonstiger Verluste, die nicht die Folgen von Personen- oder Sachschäden sind.

Unternehmen können entsprechenden Schadenersatzforderungen von Kunden etwa dann ausgesetzt sein, wenn sie eine Fertigungsanlage geliefert haben, bei der sich im laufenden Betrieb herausstellt, dass die Anlagenjustierung nicht stabil bleibt, und wenn dann infolge der notwendigen Nachjustierung ein Produktionsausfall (ohne vorausgehenden Sachschaden) auftritt.

23.4.4 Weiterfresserschäden

Ein sogenannter Weiterfresserschaden liegt vor, wenn ein Fehler an einem funktionell abgrenzbaren Teil einer gelieferten Gesamtsache dazu führt, dass diese nach Auslieferung

beim Kunden zerstört oder beschädigt wird. Eine Haftung kann sich hier gemäß der obergerichtlichen Rechtsprechung aus § 823 BGB ergeben.

Entsprechende Schadenszenarien sind zum Beispiel für Versicherungsnehmer aus dem Maschinenbau von Bedeutung. So werden Maschinen von Unternehmen aus verschiedenen Einzelteilen hergestellt. Kommt es nach Verkauf und Abnahme einer Maschine aufgrund eines mangelhaften Einzelteils zu einem Sachschaden an der Maschine, besteht im Rahmen einer klassischen Betriebs-Produkthaftpflichtversicherung keine Deckung für diesen Schaden. Denn Ziff. 7.8 AHB bzw. Ziff. A 1-7.6 AVB BHV (Herstellungs- und Lieferungsausschlussklausel) schließt den Versicherungsschutz für diese Ansprüche ausdrücklich aus.

Wenige Versicherer bieten derzeit eine Deckungserweiterung für Weiterfresserschäden über einen Ergänzungsbaustein zur Betriebs- und Produkthaftpflichtversicherung an. Diese Ergänzung erfasst zum Beispiel Schäden an einer vom Versicherungsnehmer gelieferten Maschine durch Explosion, Bersten, Brand oder Wassereintritt (named-perils), wenn ein mangelhaftes Einzelteil der Maschine der Auslöser war (vgl. Klinkhammer 2015, S. 4).

23.5 Weiterentwicklungen und Innovationen

Infolge des kontinuierlichen Technologiefortschritts können bei Unternehmen neuartige Risiken entstehen oder es können sich aktuelle Risikoverhältnisse signifikant verändern. Insbesondere wird die Digitalisierung die Gesellschaft und damit auch die Arbeitswelt nachhaltig beeinflussen. Vernetzte Produktionstechniken, automatisierte Verwaltungsvorgänge und der Einsatz künstlicher Intelligenz (KI) sind nur einige Beispiele in diesem Zusammenhang.

Die digitale Entwicklung hin zur selbstorganisierenden Produktion und dem Internet of Things (IoT) wird auch als die vierte industrielle Revolution (Industrie 4.0) bezeichnet. In der produzierenden Industrie geht es zum Beispiel um miteinander kommunizierende und lernende Maschinen oder um 3-D-Printing, also Technologien, die einen einschneidenden Einfluss auf die Art und Wirksamkeit von Produktionsprozessen haben können. Im Dienstleistungssektor erlaubt die Digitalisierung von Geschäftsprozessen andere Arten des Kundenzugangs, etwa durch die Entwicklung neuer Kundenportale und den erweiterten Einsatz sozialer Medien.

Alle Aspekte der Digitalisierung in Industrie und Wirtschaft, sowohl in technologischer Hinsicht als auch mit Blick auf die Mitarbeiter, die die Digitalisierung vorantreiben, wirken sich effektiv auf die Risikosituation in den betroffenen Unternehmen aus (vgl. Mahnke 2018, S. 4).

Das Auftauchen neuartiger Risikofelder, die im Rahmen versicherungstechnischer Bewertungen auch als „Emerging Risks“ bezeichnet werden, wirft auf Seiten der Versicherungsnehmer vor allem auch die Frage auf, ob in dieser Hinsicht ausreichender Versicherungsschutz besteht oder sichergestellt werden kann.

Neuartigen Deckungsbedarf angemessen zu befriedigen und eine möglichst weitgehende Kongruenz zwischen Haftung und Haftpflichtversicherung zu ermöglichen bzw. aufrechtzuerhalten, entspricht der berechtigten Erwartungshaltung der Unternehmen an ihre Versicherer. Diverse neuere Haftpflichtversicherungsprodukte, wie sie etwa unter der Bezeichnung „Tech E&O“ oder „ICT Pro Tech“ anzutreffen sind, weisen hier in die richtige Richtung.

Im Folgenden werden einige der neuartigen Entwicklungen kurz illustriert, wobei die unter Abschn. 23.5.1 behandelten Aspekte der Künstlichen Intelligenz (KI) in die in Abschn. 23.5.2, 23.5.3 und 23.5.4 aufgeführten Bereiche hineinwirken.

23.5.1 Künstliche Intelligenz

Künstliche Intelligenz (KI) ist laut Wikipedia ein Teilgebiet der Informatik, welches sich mit der Automatisierung intelligenten Verhaltens und mit dem maschinellen Lernen befasst. Der Begriff ist insofern nicht eindeutig abgrenzbar, als es bereits an einer genauen Definition von „Intelligenz“ mangelt. Dennoch wird der Begriff KI in Forschung, Wissenschaft und Entwicklung allgemeinhin verwendet.

Unter KI kann man Methoden verstehen, die es einem Computer ermöglichen, solche Aufgaben zu lösen, die, wenn sie vom Menschen gelöst werden, Intelligenz erfordern.

Die im Folgenden noch näher behandelten Bereiche (Robotik, Autonomes Fahren) sind aktuelle Einsatzfelder von KI.

Durch die Verlagerung von Arbeitsabläufen auf Maschinen und KI ohne unmittelbare Einwirkungsmöglichkeit des Menschen stellt sich auch die Frage nach der Übernahme einer Verantwortung für Fehler und Schäden. Auch seitens des Gesetzgebers wird unter anderem die Frage diskutiert, ob Maschinen und Anlagen, die mit KI ausgestattet selbstständig interagieren können, eine Rechtspersönlichkeit benötigen, damit die Interaktion rechtswirksam erfolgen und im Falle eines Verstoßes eine Zuordnung der Verantwortung vorgenommen werden kann (vgl. auch Abschn. 23.5.2).

Wie der Versicherungsschutz eines Unternehmens bezüglich der Auswirkungen neuartiger Risiken einzuschätzen ist, geht mit der Frage einher, ob ein neuartiges Risiko unter den Oberbegriff des versicherten Risikos (im Sinne einer primären Risikoabgrenzung) der jeweiligen Deckung fällt oder nicht. Immer dann, wenn ein solches Risiko eher in abstrakter als in konkret beschreibbarer Ausprägung vorliegt, sollte es grundsätzlich unter das versicherte Risiko subsummiert werden können (vgl. Torbohm 2018, S. 8).

Ob das betrachtete Risiko im Wege der sekundären Risikobegrenzung durch einen Ausschluss aus der Deckung fällt oder nicht, ist einzelfallbezogen zu beurteilen. Ob ein grundsätzlich bejahter Versicherungsschutz im Hinblick auf die konkret zu erwartende Schadensart tragfähig ist, hängt auch von der konkreten Schadenart sowie der vereinbarten Deckung ab (zum Beispiel Industrie 4.0: Deckung für Personen- und Sachschäden, jedoch eingeschränkte Deckung für reine Vermögensschäden).

Neben der Schadenart spielt für den Versicherungsschutz bei neuartigen Risiken ferner die Versicherungsfalldefinition eine Rolle. Je ausgeprägter der Long-Tail-Charakter eines Risikos ist, desto größer kann die Herausforderung werden, für zukünftige Versicherungsfälle eine tragfähige Deckung sicherzustellen.

Im Rahmen der Haftpflichtversicherung sind Deckungserweiterungen, wie die in den AHB umfasste Vorsorgeversicherung und auch der Versicherungsschutz für Erhöhungen und Erweiterungen versicherter Risiken, für den Versicherungsnehmer vorteilhaft. Allerdings steht dem Versicherer ggf. für den Fall, dass eine Risikoerhöhung durch die Änderung bestehender oder den Erlass neuer Rechtsvorschriften eintritt, ein Kündigungsrecht zu.

Schließlich ist noch zu beachten, dass die Bestimmungen der §§ 23 ff. VVG dem Versicherer auf der Prämien- und Bedingungsseite bestimmte Handlungsmöglichkeiten für eingetretene Gefahrerhöhungen nach Vertragsschluss einräumen.

23.5.2 Robotik

Unternehmen verfügen hierzulande über eine hohe Dichte an Robotern. Als Industrieroboter werden programmierbare Maschinen bezeichnet, die zur Handhabung, Montage oder Bearbeitung von Werkstücken im industriellen Umfeld eingesetzt werden. Diese Roboter bestehen zum Großteil aus einem Roboterarm, einem Greifer, diversen Sensoren sowie einer Steuerungseinheit. Sie können Aktionen entsprechend ihrer Programmierung auch autonom ausführen.

Das Thema Robotik stellt auch die Haftpflichtversicherer vor Herausforderungen, sei es, dass ihre Versicherungsnehmer Roboter herstellen oder dass die Versicherungsnehmer Robotik für betriebliche Zwecke einsetzen.

Neben Industrierobotern werden zunehmend auch humanoide Formen eingesetzt, etwa im Umgang mit Endverbrauchern, wenn es zum Beispiel um Auskunftserteilung geht.

Wenn ein Roboter bei diesen Betätigungen falsch handelt, stellt sich die Frage, wer dafür haftet, zum Beispiel der Programmierer, der Hersteller oder der Nutzer.

Nach dem derzeit geltenden Recht haftet grundsätzlich die natürliche oder juristische Person, der die Verursachung eines Schadens zuzurechnen ist. Da ein Roboter keine derartige Person ist, kann er nach geltendem Recht nicht verantwortlich sein.

Damit richtet sich der Blick vorrangig auf die Verantwortlichkeit des Herstellers nach den Grundsätzen der Produkthaftung. Fährt also zum Beispiel der Rasenmäher-Roboter dem Besitzer über den Fuß und verletzt diesen, haftet grundsätzlich der Hersteller.

Wenn der Roboter aber nicht nur mit einem einfachen Verhaltensmuster ausgestattet ist wie im Falle des Rasenmähers, sondern über selbstlernende Elemente verfügt, also über KI, ist die klassische Fehlerzuweisung zu hinterfragen. Denn je selbstlernender eine KI ist, desto autarker und unvorhersehbarer für Hersteller oder Programmierer sind ihre Ergebnisse und Entscheidungen.

Die Handlung eines intelligenten, selbstlernenden Roboters, sei es im Verbraucher- oder im Industrie-Umfeld, könnte künftig also weit von dem entfernt sein, was ihm ursprünglich durch die Programmierung beigebracht wurde. Damit werden hinsichtlich der Haftung neue Fragen aufgeworfen. So wird zum Beispiel diskutiert, ob einem Roboter eine (Teil-)Rechtsfähigkeit und damit der Status einer elektronischen Person (E-Person) zugebilligt werden soll.

Fest steht allerdings, dass derzeit sowohl das Produkthaftungsgesetz als auch die Produzentenhaftung gemäß BGB geeignete Grundlagen für den Geschädigten bilden können, um seine Ansprüche geltend zu machen. Diese gesetzlichen Ansprüche gehören zu denjenigen Risiken, für die der Hersteller in der Regel Produkthaftpflichtversicherungsschutz vereinbart hat.

23.5.3 Drohnen

Drohnen erfreuen sich immer größerer Beliebtheit. Das gilt nicht nur für den Privatbereich, sondern auch für das industrielle Umfeld. Dort werden Drohnen zum Beispiel zu Forschungszwecken, zur Überwachung von Industrieanlagen, Pipelines oder Stromleitungen, zur Sichtung von Flächen, für Foto- und Filmaufnahmen oder für Logistikdienstleistungen eingesetzt.

Stürzt eine Drohne ab, haftet der Halter gemäß Luftverkehrsgesetz (LuftVG) verschuldenunabhängig für die Schäden Dritter. Für die Nutzung von Drohnen besteht in Deutschland eine Versicherungspflicht. Diese gilt unabhängig davon, ob eine Drohne privat oder gewerblich genutzt wird.

Die Herausforderung für Versicherer besteht hierbei darin, dass sie Risiken bewerten und Deckungen vergeben müssen, ohne dass sie über entsprechende historische Schadendaten verfügen. Deshalb entwickelt sich der Markt für den Versicherungsschutz von Drohnen bisher langsam.

Einige spezialisierte Versicherer haben ein gewisses Portfolio von Drohnendeckungen im Rahmen der Luftfahrtversicherung aufgebaut. Die Versicherungssummen bewegen sich meist im Bereich von ein bis zehn Millionen Euro.

In Einzelfällen kann das Haftpflichtrisiko unter Vereinbarung individueller Regelungen auch in eine bestehende Betriebs- oder Produkthaftpflichtpolice eingeschlossen werden.

23.5.4 Autonomes Fahren

Auch bei den vielfältigen technologischen Fragestellungen im Zusammenhang mit autonomem Fahren (zum Beispiel automatisierte Autos) spielt KI (vgl. Abschn. 23.5.1) eine bedeutende Rolle.

Aufgrund massiver Investitionen und technologischer Fortschritte werden autonome Fahrzeuge immer zahlreicher und leistungsfähiger und kommen in vielfältigen Umgebun-

gen zum Einsatz. Dies reicht von teilautonomen bis zu vollständig selbstfahrenden Pkw, Taxis, Bussen und Lkw, die im öffentlichen Straßenverkehr eingesetzt werden, über Shuttles, die Menschen in geschlossenen Umgebungen wie Flughäfen und Campusanlagen befördern bis hin zu automatisierten Gabelstaplern, die Waren im Bereich von Vertriebszentren und Produktionsbetrieben transportieren.

Der Gesetzgeber hat im Straßenverkehrsgesetz einschlägige Regelungen getroffen (vgl. Seidl 2018, S. 9): Die Autos, die bis jetzt auf der Straße fahren, bewegen sich teilautomatisiert im Rahmen zwischen „Level 0“ und „Level 2“. Für den Fahrer bedeutet das: Er kann und muss die Systeme überwachen, die Kontrolle behalten und ggf. jederzeit in das Handeln der Systeme eingreifen bzw. auf Aufforderungen des Systems reagieren können.

Zur Haftung bei Unfällen mit teilautomatisierten Autos gilt zunächst (vgl. Pütz 2019, S. 9): Der Halter haftet nach den Grundsätzen der Gefährdungshaftung. Deswegen braucht auch jeder Fahrzeughalter eine Kfz-Haftpflichtversicherung. Kann sich der Fahrzeughalter im Falle eines Schadensereignisses nicht ausnahmsweise auf den seltenen Haftungsausschluss der höheren Gewalt berufen, haftet er grundsätzlich für alle Unfallschäden, auch solche, die auf Grund von Fehlern des Autos oder wegen der falschen Bedienung von softwaregesteuerten Fahrzeug- bzw. teilautonomen Fahrerassistenzsystemen entstehen.

Der Fahrer haftet bei einem Unfall für vermutetes Verschulden. Das Gesetz geht also davon aus, dass er Schuld hatte, er kann diese Vermutung aber entkräften. Gelingt ihm dies nicht, haftet auch er für alle Schäden, die Dritten entstanden sind, also auch für solche, die von softwaregesteuerten Systemen (mit-)verursacht wurden.

Der Kfz-Haftpflichtversicherer kann ggf. beim Fahrer oder beim Hersteller des automatisierten Fahrzeugsystems Ressort nehmen.

Daneben gibt es die verschuldensunabhängige Produkthaftung (Gefährdungshaftung). Danach haben Fahrzeughalter einzutreten, wenn durch einen technischen Fehler des Fahrzeugs jemand getötet wurde, Körper- oder Gesundheitsverletzungen eingetreten sind oder andere Sachen als das Fahrzeug selbst beschädigt wurden. Dabei kann ein Hersteller auch für Fehler von Zulieferern haften, zum Beispiel bei Fehlern in einer verwendeten Software.

Schließlich gibt es noch die verschuldensabhängige Produzentenhaftung nach § 823 BGB, die eingreift, wenn der Hersteller zum Beispiel ein Produkt nicht zurückgerufen hat, nachdem Sicherheitsrisiken bekannt geworden sind, oder wenn er die Fahrer nicht auf riskante Änderungen durch Software-Updates aufmerksam gemacht hat.

Die Stufen ab „Level 3“ gelten für das hoch- und voll automatisierte Fahren. Beim hochautomatisierten Fahren darf sich der Fahrer zeitweise anderen Tätigkeiten zuwenden. Das System muss aber durch den Fahrer jederzeit per Hand übersteuerbar oder deaktivierbar sein. Außerdem muss es rechtzeitig Ton- oder Lichtsignalen anzeigen, wenn das nötig ist. Experten erwarten solche Fahrzeuge frühestens für 2020 auf dem Markt.

Die Vollautomatisierung, „Level 4“, bei der der Fahrer nur noch im Notfall eingreifen muss, wird wohl erst noch später serienreif werden. Und „Level 5“, das eigentliche autonome Fahren, bei dem Menschen nur noch Passagiere sind, ist bislang noch Zukunftsmusik.

Der Fahrer darf sich dem Gesetz zufolge bei der hoch- und voll automatisierten Fahrt (Level 3 und 4) vom Verkehrsgeschehen und der Fahrzeugführung abwenden. Er darf also die Hände vom Lenker nehmen und kann sogar im Internet surfen, solange er nur weiter am Lenkrad sitzt. All die Ablenkungen durch elektronische Medien, die gerade für herkömmliche Autos verboten wurden, sind für solche Autos explizit erlaubt. Wichtig ist aber, dass der Fahrer in der Lage bleibt, jederzeit selbst wieder unverzüglich zu übernehmen. Dies muss er nach dem Gesetz entweder tun, wenn das hoch- oder voll automatisierte System ihn dazu auffordert, oder wenn er erkennt oder aufgrund offensichtlicher Umstände erkennen muss, dass er dringend eingreifen muss, weil das voll automatisierte Fahren nicht mehr funktioniert.

An der Halterhaftung bei Unfällen mit einem allein fahrenden Fahrzeug ändert sich auch zukünftig grundsätzlich nichts, denn es gilt weiter die Gefährdungshaftung. Allerdings dürfte sich der Kfz-Haftpflichtversicherer bei Autos, die mindestens „Level 3“ beherrschen, zukünftig leichter an den Autohersteller wenden können. Der Fahrer haftet zum Beispiel dann, wenn er die Aufforderung des Systems ignoriert hat, wieder das Steuer zu übernehmen.

Vor diesem Hintergrund müssen alle Autos, die die höheren Levels beherrschen, einen Unfalldatenspeicher (Black Box) an Bord haben. Der Fahrer wird damit permanent überwacht. Hier wird dann der Datenschutz besonders wichtig. Außerdem steigt damit die Gefahr, dass Hacker von außen die Kontrolle über ein Fahrzeug übernehmen und bewusst Unfälle provozieren können.

Während die Sicherheitsvorteile mobiler Autonomie wahrscheinlich erheblich sein werden, rücken die Fragen des Risikomanagements und die Auswirkungen auf Unternehmen in diesem Umfeld, einschließlich Fahrzeughersteller, Komponentenhersteller und Softwareentwickler, stärker in den Fokus. Bisweilen wird prognostiziert, dass Produktrückrufe in der Automobilindustrie angesichts der komplexen Technologien und der unterschiedlichen Einsatzmöglichkeiten der Fahrzeuge noch mehr an Bedeutung gewinnen könnten. Damit ist wiederum auch die Betriebs- und Produkthaftpflichtversicherung insofern angesprochen, als Unternehmen an eine dort „anknöpfbare“ Rückrufkosten-Haftpflichtversicherung denken sollten.

23.5.5 Fazit

Die aufgezeigten Entwicklungen in Gesellschaft und Arbeitswelt, die mit den Begriffen Digitalisierung, Industrie 4.0 und KI nur ansatzweise umschrieben werden können, sorgen dafür, dass die Betriebs- und Produkthaftpflichtversicherung ihre Stellung als wesentliche Säule des betrieblichen Versicherungsschutzes auch künftig beibehält.

Literatur

- Bauer A. (2019). Überlegungen zu Risiken, Schäden und Versicherungen im energiewirtschaftlichen Umfeld. *Die Versicherungspraxis*, 2019(1), 3–6.
- Czeremuga C. (2017). Versicherungsrechts-Tipp „Was richtig erprobt ist, geht nicht kaputt!“ – Vertheidigungsstrategien gegen den Einwand der mangelnden Erprobung. *Die VersicherungsPraxis*, 2017(9), 40–46.
- Dengler, M. (1999). *Die Haftpflichtversicherung im privaten und gewerblichen Bereich* (2. Aufl.). München: C.H. Beck.
- Klinkhammer, G. (2015). Innovationen in der Industrie-Haftpflichtversicherung – und sie bewegen sich doch (nicht?). *Die VersicherungsPraxis*, 2015(9), 3–9.
- Littbarski, S. (2014). *Produkthaftpflichtversicherung, Kommentar* (2. Aufl.). München: C.H. Beck.
- Mahnke, A. (2018). Die Digitalisierung im Umfeld der Industriever sicherung – Eine Standortbestimmung. *Die VersicherungsPraxis*, 2018(5), 3–6.
- Nickel, F., & Nickel-Fiedler, A. (2015). *Produkt-Haftpflichtversicherungsrecht* (2. Aufl.). Berlin: Erich Schmidt.
- Prölls, J., Martin, A., & Voit, W. (2018). *Versicherungsvertragsgesetz* (30. Aufl.). München: C.H. Beck.
- Pütz, F. (2019). Führt das automatisierte Fahren zu einer materiellen Verlagerung von Haftungskosten auf die Herstellerseite. *Die VersicherungsPraxis*, 2019, 8–12.
- Schimikowski, P. (2015). OLG Koblenz, 17.03.2014 – 10 U 1170/13: Betriebshaftpflichtvers.: Bewusst pflichtwidriges Verhalten eines Kranführers (m. Anm. Schimikowski), in r+s 5/15, S. 231–232. München: C.H. Beck.
- Seidl, M. (2018). Wer haftet in der digitalen Welt? Die Frage der Verantwortung für Schäden am Beispiel „Autonomes Fahren“. *Die VersicherungsPraxis*, 2018, 7–9.
- Seiring, J., Kraus, H., & Steinberger, C. (2016). *Produkthaftung* (6. Aufl.). Frankfurt a. M.: VDMA.
- Späte, B., & Schimikowski, P. (2015). *Haftpflichtversicherung, Kommentar zu den AHB und weiteren Haftpflichtversicherungsbedingungen* (2. Aufl.). München: C.H. Beck.
- Thürmann, D., & Kettler, C. (2009). *Produkthaftpflichtversicherung und ausgewählte Fragen der Produkthaftung* (6. Aufl.). Karlsruhe: Versicherungswirtschaft GmbH.
- Torbohm, L. (2018). Emerging Risks-Herausforderung für das Risikomanagement von Industrieunternehmen. *Die VersicherungsPraxis*, 2018, 3–8.

Georg Klinkhammer ist Rechtsanwalt. Von 1986 bis 2018 war er beim GVNW e. V. (vormals DVS e. V.) als Referent für Haftpflicht- und Financial Lines-Versicherungen angestellt. Neben der Beratung von Mitgliedsunternehmen zählten Vortrags- und Seminartätigkeiten sowie Veröffentlichungen in der Fachzeitschrift VersicherungsPraxis und in anderen Fachpublikationen zu seinem Aufgabenbereich. Seit 2010 war Georg Klinkhammer zudem Syndikus des Verbandes.

Harald Kurtze studierte Versicherungswesen mit den Schwerpunkten Rückversicherung, Organisation und Informationsverarbeitung des Versicherungsbetriebs, Bilanzierung von Versicherungsunternehmen und Sachversicherung am Institut für Versicherungswesen der Technischen Hochschule Köln. Im Anschluss absolvierte er dort auch das Masterstudium Risk & Insurance. Neben dem Studium war bei der Kölner Forschungsstelle Rückversicherung als Wissenschaftlicher Mitarbeiter tätig und erwarb den Titel des Fellow of the Chartered Insurance Institute in London (FCII).



Financial Lines – D&O-Versicherung

24

Marcel Wilms und Christopher Schatz

Zusammenfassung

Dieses Kapitel vermittelt dem Leser einen Überblick über die D&O-Versicherung (Directors-and-Officers-Versicherung). Sie wird auch als Vermögensschaden-Haftpflichtversicherung von Aufsichtsräten, Vorständen und Geschäftsführern, Organ- oder Manager-Haftpflichtversicherung bezeichnet und bietet den Unternehmensleitern Schutz vor einer persönlichen Inanspruchnahme wegen einer tatsächlichen oder vermeintlichen Pflichtverletzung als Organ einer Gesellschaft. Dabei orientiert sich dieses Kapitel an den Musterbedingungen des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV) für die D&O-Versicherung, den „Allgemeine Versicherungsbedingungen für die Vermögensschaden-Haftpflichtversicherung von Aufsichtsräten, Vorständen und Geschäftsführern (AVB D&O)“, Stand Mai 2019. Diese Bedingungen sind für die Versicherungsunternehmen unverbindlich und ihre Verwendung ist rein fakultativ. Viele Versicherer nutzen abweichende Bedingungen. Hinzu kommen sogenannte „Maklerwordings“, also von Versicherungsmaklern entwickelte oder weiterentwickelte Versicherungsbedingungen sowie Individualvereinbarungen.

Es wird zunächst kurz auf die Entwicklung der D&O-Versicherung eingegangen, um anschließend den Umfang der D&O-Versicherung darzustellen. Der Umfang gliedert sich in den Gegenstand der Versicherung, den zeitlichen, sachlichen und örtlichen Umfang sowie die Ausschlüsse. In der gebotenen Kürze können nicht alle Regelungen

M. Wilms (✉)

Gothaer Allgemeine Versicherung AG, Köln, Deutschland

E-Mail: marcel_wilms@gothaer.de

C. Schatz

TH Köln, Institut für Versicherungswesen, Köln, Deutschland

E-Mail: chris.schatz1996@googlemail.com

einer D&O-Versicherung erschöpfend dargestellt werden. Die allgemeinen Regelungen zum Beginn des Versicherungsschutzes und der Beitragszahlung, der Dauer und dem Ende des Vertrages einschl. der Kündigung, zur Anzeigepflicht, Gefahrerhöhung, anderen Obliegenheiten sowie zu einigen weiteren Vertragsregelungen werden im Hinblick auf den Umfang der Darstellung nicht erläutert.

24.1 Einführung

Die persönliche Haftung von Unternehmensleitern gewinnt weltweit immer weiter an Bedeutung. Unternehmensleiter können sich sowohl im Innenverhältnis gegenüber ihrem eigenen Unternehmen wie auch im Außenverhältnis gegenüber Dritten schadensersatzpflichtig machen. Die Haftung ist der Höhe nach nicht begrenzt und kann das gesamte Privatvermögen des haftenden Unternehmensleiters erfassen. In Streitigkeiten über vermeintliche oder tatsächliche Pflichtverletzungen können allein die Abwehrkosten finanzielle Dimensionen erreichen, welche die persönlichen Vermögensverhältnisse der Unternehmensleiter überfordern.

Kein Unternehmensleiter, auch nicht ein noch so sorgfältig handelnder Vorstand oder Geschäftsführer, kann ausschließen, dass es im Einzelfall zu einer Fehlentscheidung kommt, die sich bei späterer Bewertung als fahrlässige Pflichtverletzung erweist. Die D&O-Versicherung bietet den Unternehmensleitern eine Absicherung gegen die Folgen von Pflichtverletzungen, indem sie die versicherten Personen im Falle einer persönlichen Inanspruchnahme von berechtigten Ansprüchen freistellt und unberechtigte Ansprüche sowohl gerichtlich als auch außergerichtlich abwehrt. Eine D&O-Versicherung gehört heute zum Manager wie eine Vermögenshaftpflichtversicherung zu Steuerberatern oder Rechtsanwälten, oder wie die Heilwesenhaftpflichtversicherung zum Beruf des Arztes.

Der D&O Versicherungsmarkt stellt sich seit seinem Entstehen in Deutschland Mitte der achtziger Jahre des letzten Jahrhunderts als sehr vielfältig dar. Die Bedarfe und Versicherungsmöglichkeiten von Unternehmensleitern kleinerer und mittlerer Unternehmen gegenüber dem Versicherungsbedarf multinationaler (börsennotierter) Großunternehmen oder von Familienunternehmen können sich teils erheblich voneinander unterscheiden.

24.2 Zweck der D&O-Versicherung

Zweck der D&O-Versicherung ist der Schutz der Unternehmensleiter sowie der Gesellschaft selbst. Darüber hinaus sollen auch das Aktionärs- und Gläubigervermögen geschützt werden (vgl. Dreher, 2005, S. 1670).

Manager haften mit ihrem gesamten privaten Vermögen für Vermögensschäden, die sie durch eine Pflichtverletzung verursachen. Ohne eine D&O-Versicherung besteht die Gefahr, dass das Privatvermögen des Unternehmensleiters den durch eine Pflichtverletzung

entstandenen Schaden nicht abdeckt (vgl. Säcker 2005, S. 10). Der Geschädigte bleibt auf dem Schaden sitzen. Das kann auch das Unternehmen treffen, dessen Organ der Manager ist. Die D&O-Versicherung schützt deshalb immer auch das Vermögen der Gesellschaft.

Ferner soll der Versicherungsschutz den Managern die Sicherheit vermitteln, die sie für ihre unternehmerische Handlungsfähigkeit benötigen. Sie sollen keine Haftungsansprüche fürchten müssen, sondern sich auf ihre Tätigkeiten im Unternehmen konzentrieren können.

24.3 Entwicklung der D&O-Versicherung

In Deutschland wurde bereits Ende des 19. Jahrhunderts ein erstes Versicherungskonzept zur Absicherung von Aufsichtsratsmitgliedern gegen Haftpflichtansprüchen angeboten. Auf Aufforderung des preußischen Innenministers wurde das Geschäft allerdings bereits 1896 wiedereingestellt. Der D&O-Versicherungsgedanke geriet daraufhin in Deutschland für lange Zeit in Vergessenheit (vgl. Ihlas 2017, Rn. 2). Erst in den 1980er-Jahren wurde er in Deutschland wieder aufgegriffen.

In der Weltwirtschaftskrise Ende der 1920er-Jahre, die mit dem New Yorker Börsencrash im Oktober 1929 begann, wurde in den USA die Haftung für Manager gegenüber Aktionären verschärft. In der Folge kamen in den 1930er-Jahren die ersten D&O-Versicherungen in den USA auf. Mit dem Anstieg von Haftungsfällen und der Anerkennung der Prämienzahlung durch das Unternehmen nahm die Verbreitung in den 1960er- und 1970er-Jahren zu (vgl. Ihlas 2009, S. 91 f.). In den 1980er-Jahren hatten 96,8 Prozent aller an der New Yorker Börse notierten Unternehmen eine D&O-Versicherung zum Schutz ihrer Unternehmensleiter (vgl. Scheifele 1993, S. 3). Über die USA kam die Versicherungsidee zurück nach Deutschland. 1986 verkaufte die Chubb Group of Insurance Company die erste D&O Versicherung in Deutschland (vgl. Finkel und Seitz 2016, S. 43).

Die D&O-Versicherung gehört heute auch in Deutschland zum Standard der Unternehmensversicherungen. Der deutsche D&O-Versicherungsmarkt ist mittlerweile so vielfältig wie die Unternehmen, deren Leiter im Fokus des angebotenen Versicherungsschutzes stehen. Die Bedarfe und Versicherungsmöglichkeiten von Unternehmensleitern unterscheiden sich, abhängig von der Gesellschaftsform und den Eigentümerverhältnissen in den betroffenen Unternehmen, erheblich voneinander. Dem trägt der Versicherungsmarkt Rechnung und bietet hierfür unterschiedliche Lösungen an.

Das weltweite Prämienvolumen wird auf 15 Milliarden US-Dollar p.a. geschätzt (Allianz, Pressemitteilung vom 04.12.2019). Der GDV schätzt das Prämienvolumen des inländischen Direktgeschäfts in Deutschland auf rund 500 Millionen Euro zzgl. Versicherungsteuer.

Die Profitabilität der D&O-Versicherung ist aufgrund steigender Schadenzahlen und des hohen Wettbewerbs weltweit unter Beobachtung der Versicherer (Allianz, Pressemitteilung vom 04.12.2019). Zuletzt mussten die deutschen Versicherer in der D&O-Versicherung Verluste hinnehmen. Die vom GDV veröffentlichten Zahlen weisen für die Jahre 2016 bis 2018 Schadenquoten von 99,1 Prozent (2016), 85,3 Prozent (2017) und 112,9 Prozent (2018) aus. Darin sind noch keine Kosten berücksichtigt. Es melden aller-

dings nur 33 von 50 Mitgliedsunternehmen des GDV, die D&O-Versicherungen anbieten dürfen, Zahlen an den Verband.

Die Versicherer reagieren aktuell auf die negativen Ergebnisse mit Preiserhöhungen und Kürzungen der angebotenen Versicherungssummenkapazitäten.

24.4 Gegenstand der Versicherung

24.4.1 Versicherungsbausteine

Die D&O-Versicherung ist eine Vermögensschaden-Haftpflichtversicherung. Sie schützt die Unternehmensleiter vor den finanziellen Folgen von Pflichtverletzungen, die sie in Ausübung der betrieblichen Tätigkeit begehen. Die Leistung des Versicherers umfasst im Schadenfall die Prüfung, ob und in welcher Höhe der Unternehmensleiter zum Schadenersatz verpflichtet ist, sowie die Zahlung der Entschädigungsleistung an den Geschädigten, wenn Ansprüche berechtigt sind. Unberechtigte Ansprüche wehrt der Versicherer ab, das heißt, er trägt die Kosten für die Verteidigung. Dazu zählen insbesondere Rechtsanwaltskosten für außergerichtliche oder gerichtliche Streitigkeiten.

Die D&O-Versicherung deckt reine Vermögensschäden, also weder Personen- noch Sachschäden ab.

Die D&O-Versicherung unterteilt sich meist in zwei bis drei Hauptbausteine:

- die persönliche Deckung von Organmitgliedern (sogenannte Side A)
- die Deckung für das Unternehmen, wenn es ein Organmitglied von Ansprüchen Dritter freistellt (sogenannte Firmen-Enthaftungsversicherung/„Company Reimbursement“ oder Side B-Deckung) sowie
- die Deckung für das Unternehmen für den Fall einer Inanspruchnahme des Unternehmens wegen der Verletzung von Wertpapiervorschriften (sogenannte Entity- oder Side C-Deckung). Dieser Baustein gilt nur für die juristische Person. Er wird nur von einigen börsennotierten Aktiengesellschaften gekauft.

24.4.2 Versicherungsschutz für die Manager

Versicherungsschutz für die Manager wird für den Fall gewährt, dass ein Manager wegen einer bei Ausübung seiner Tätigkeit begangenen Pflichtverletzung aufgrund gesetzlicher Haftpflichtbestimmungen für einen Vermögensschaden auf Schadenersatz in Anspruch genommen wird.

Versichert ist die gesamte Tätigkeit als Geschäftsführer, Vorstands- oder Aufsichtsratsmitglied. Damit sind die gesetzlichen Aufgaben als Organ umfasst. Aus der Satzung bzw. aus dem Gesellschaftsvertrag können sich weitere Aufgaben ergeben, zum Beispiel im Rahmen einer Geschäftsordnung. Um Unklarheiten darüber zu vermeiden, ob eine Hand-

lung des Organmitgliedes eine Organitätigkeit oder ein rein „operatives Handeln“ ist, werden in vielen Versicherungsbedingungen operative Tätigkeiten ausdrücklich mitversichert.

Versicherungsschutz besteht für gesetzliche Haftpflichtbestimmungen. Darunter werden allgemein Rechtsnormen verstanden, die an die Verwirklichung eines Tatbestandes Rechtsfolgen knüpfen, die unabhängig vom Willen der beteiligen Personen eintreten (vgl. Prölss und Martin 2015, Ziffer 1 AHB Rn 6 m. w. N.). Zu beachten ist, dass damit nicht nur deliktische und quasideliktische Ansprüche umfasst sind, sondern auch gesetzliche Schadensersatzansprüche aus einer Vertragsverletzung oder eines vorvertraglichen Schuldverhältnisses.

Ansprüche gegen Geschäftsführer wegen Zahlungen nach Insolvenzreife nach § 64 GmbHG und Vorstände nach §§ 93 Abs. 3 Nr. 6 in Verbindung mit 92 Abs. 2 AktG sollten ausdrücklich in der D&O-Versicherung mitversichert werden, da diese Ansprüche in zwei OLG Entscheidungen nicht als Haftpflichtansprüche angesehen worden sind (OLG Düsseldorf vom 20. Juli 2018, Az. I-4 U 93/16 und OLG Celle vom 01.04.2016, Az. 8 W 20/16).

In den jüngeren GDV-Musterbedingungen sind auch öffentlich-rechtliche Ansprüche mitversichert. In den AVB D&O ist eine Beschränkung auf Haftpflichtansprüche „privatrechtlichen Inhalts“ nicht entfallen.

Die D&O-Versicherung bietet Versicherungsschutz sowohl für Innenhaftungs- als auch Außenhaftungsansprüche. Unter Innenhaftung versteht man die Haftung von Organmitgliedern nach Pflichtverletzungen gegenüber der Gesellschaft, die das Organmitglied beschäftigt (vgl. Schilling 2007, S. 3). Unter Außenhaftung versteht man die Haftung gegenüber Dritten, zum Beispiel Gläubigern der Gesellschaft, Aktionären, Anlegern und sonstigen Dritten wie Fiskus oder Sozialversicherungen (vgl. Schüppen und Schaub 2010, § 24, Rn. 47). Geschädigte und Anspruchssteller gegenüber der versicherten Person können bei Innenansprüchen die Gesellschaft selbst, bei Außenhaftungsansprüchen aber auch Dritte sein (vgl. Finkel und Seitz 2016, S. 47).

Eine Außenhaftung des Geschäftsführers, also die Haftung des Geschäftsführers gegenüber einem Dritten, kann sich aus unterschiedlichsten Gründen ergeben, zum Beispiel aus unerlaubten Handlungen, für nicht abgeführte Arbeitnehmeranteile zur Sozialversicherung oder auch aus dem Steuerschuldverhältnis des Unternehmens. Auch die Fortführung des Unternehmens nach Eintritt der Insolvenzreife kann zu einer Haftung führen. Eine persönliche Haftung der Geschäftsführer einer GmbH oder der Vorstände einer AG kann für Zahlungen entstehen, wenn sie diese nach Eintritt der Zahlungsunfähigkeit oder Überschuldung noch veranlasst oder zugelassen haben (vgl. § 64 S. 1 GmbH und § 92 Abs. 2 S. 1 AktG). Da der Begriff der Zahlungen sehr weit ausgelegt wird und nicht lediglich Geldleistungen im Sinne einer Bargeldzahlung oder bargeldlosen Zahlung durch Überweisung erfasst, sondern auch andere Leistungen, wenn dadurch Liquidität zu Lasten des Gesellschaftsvermögens entzogen wird, ist das Haftungspotenzial hieraus erheblich. Es sind grundsätzlich auch die Erbringung von Dienstleistungen oder Warenlieferungen, die Herausgabe ungesicherter Gegenstände an Gläubiger, die Abtretung von Forderungen etc. erfasst. Praxisrelevant sind insbesondere auch Zahlungen Dritter auf ein debitorisch

geführtes Girokonto bei einer Bank, weil darin eine Zahlung der kriselnden Gesellschaft an die Bank gesehen wird.

Eine Innenhaftung der Vorstandsmitglieder einer Aktiengesellschaft kann sich zum Beispiel aus § 93 AktG ergeben. Vorstandsmitglieder einer Aktiengesellschaft sind nach § 93 Abs. 1 S. 1 AktG dazu verpflichtet, bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Das GmbH-Gesetz enthält in § 43 Abs. 1 GmbHG eine fast wortgleiche Regelung. Die Entscheidungen der Vorstandsmitglieder und auch der Geschäftsführer müssen immer das Gesellschaftswohl im Sinn haben. Davon dürfen sie nur dann ausgehen, wenn ihre Entscheidung auf Basis ausreichender Informationen und bewährter betriebswirtschaftlicher und kaufmännischer Grundregeln nachvollziehbar im besten Sinne des Unternehmens getroffen wird (vgl. BGH Urteil vom 21.04.1997, Az. II ZR 175/95). Andernfalls machen sich die Vorstände oder Geschäftsführer gegenüber der Gesellschaft schadensersatzpflichtig (vgl. § 93 Abs. 2 S. 1 AktG bzw. § 43 Abs. 2 GmbHG). In § 93 Abs. 2 S. 2 AktG ist zudem eine Beweislastumkehr verankert, wonach das Vorstandsmitglied beweisen muss, dass es die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters angewandt hat, wenn dies streitig ist. Schließlich finden sich in § 93 Abs. 3 AktG einige Beispiele von Handlungen, die eine Schadensersatzpflicht auslösen.

Die D&O-Versicherung deckt beide Fallgruppen, nämlich Innenhaftungs- und Außenhaftungsansprüche ab. Die ehemalige Beschränkung des Versicherungsschutzes auf Außenhaftungsansprüche ist in den GDV Musterbedingungen AVB-AVG 2013 erstmalig entfallen. Für die USA gelten Sonderregelungen.

Beispiele für Schadenereignisse sind (vgl. Zimmermann 2016):

Innenhaftungsfälle

- Verkauf von Tochtergesellschaften unter Wert,
- fehlerhafte Arbeitsanweisungen,
- mangelhafte Liquiditätskontrollen,
- Kreditgewährung ohne Sicherheiten,
- Bürgschaft ohne Gesellschafterbeschluss,
- Falschverwendung von Fördermitteln,
- Einstellung unqualifizierter Mitarbeiter,
- Offenlegung von Betriebsgeheimnissen,
- Kauf ungeeigneter Maschinen.

Außenansprüche

- Verstoß gegen Wettbewerbs-/Markenrechte,
- Ansprüche des Insolvenzverwalters,
- Nichtabführung von Sozialversicherungsbeiträgen,
- Ansprüche des Fiskus.

24.4.3 Versicherungsschutz für das Unternehmen, wenn es einen Manager freistellt

Besteht eine Verpflichtung der Versicherungsnehmerin oder einer Tochtergesellschaft, versicherte Personen für den Fall, dass diese von Dritten, also nicht von der Versicherungsnehmerin oder einer Tochtergesellschaft oder einer anderen versicherten Person haftpflichtig gemacht werden, freizustellen (Company Reimbursement), so kommt nicht mehr der Manager in den Genuss des Versicherungsschutzes, sondern das Unternehmen direkt. Der Anspruch auf Versicherungsschutz aus der D&O-Versicherung geht in dem Umfang von den versicherten Personen auf die Versicherungsnehmerin oder ihre Tochtergesellschaft über, in welchem diese die versicherten Personen freistellt. Es wird die Freistellung einer versicherten Person durch die Versicherungsnehmerin oder durch ein Tochterunternehmen abgedeckt. Die Versicherungsnehmerin oder eine Tochtergesellschaft wird Begünstigter des Versicherungsvertrags. Diese sogenannte Side-B-Deckung darf nicht fehlen, da ansonsten die Leistungen aus dem Versicherungsvertrag nur der versicherten Person zustehen (vgl. § 44 Abs. 1 VVG).

Die Company-Reimbursement-Klausel folgte aus dem Konzept der in den USA bekannten Freistellungsverpflichtungen. Voraussetzung für den Übergang des Versicherungsschutzes ist, dass die Freistellungsverpflichtung nach Art und Umfang rechtlich zulässig ist. Der Begriff der Freistellung wird in den Policien nicht weiter definiert. Die versicherungsnehmende Gesellschaft begleicht Ansprüche der Gläubiger gegenüber einer versicherten Person und stellt diese somit von der Haftpflichtschuld frei (vgl. Ihlas 2017, Rn. 63). Ursprünglich waren die AVB-AVG so ausgearbeitet, dass die Side B-Deckung eine Zusatzvereinbarung darstellte und die D&O-Versicherung somit ohne eine solche Vereinbarung eine „Side A only“-Versicherung war (vgl. Ihlas 2017, Rn. 64). Das findet man in Deutschland heute nur noch selten.

24.4.4 Versicherungsschutz für das Unternehmen bei Wertpapierhandelsansprüchen (sogenannte Side C-Deckung)

D&O-Versicherungen von börsennotierten Unternehmen enthalten zum Teil Versicherungsschutz für den Fall einer Inanspruchnahme des Unternehmens wegen der Verletzung von wertpapierhandelsgesetzlichen Bestimmungen, sogenannte „Side C“-Deckung. Andere Bezeichnungen für die Side-C-Deckung sind „Entity Coverage“ oder „SEC-Entity-Coverage“ (vgl. Ihlas 2017, Rn. 77). Anders als bei der Side-A-Deckung, also der Deckung von Ansprüchen gegenüber der versicherten Person, und der Side-B-Deckung, also der Deckung von Ansprüchen, die auf die Versicherungsnehmerin übergegangen sind, deckt die Side-C-Deckung Ansprüche gegenüber der Versicherungsnehmerin selbst. In diesem Fall ist ausschließlich die Versicherungsnehmerin Begünstigte. Der Versicherer

stellt hier die Versicherungsnehmerin von begründeten Ansprüchen frei und wehrt unbegründete Ansprüche ab. Leistungen des Versicherers, die unter der Side-C-Deckung im Hinblick auf das Unternehmen erfolgen, werden auf die Versicherungssumme der D&O-Versicherung angerechnet. Sie reduzieren also die Versicherungssumme, die auch für den Schutz des persönlichen Vermögens der versicherten Manager zur Verfügung steht.

24.5 Beteiligte

24.5.1 Versicherungsnehmerin

Das Unternehmen schließt typischerweise die D&O-Versicherung für seine Organmitglieder ab. Versicherungsnehmerin ist das Unternehmen.

Eine Nennung möglicher Versicherungsnehmer liegt in den Musterbedingungen des GDV nicht vor. Es ist dementsprechend eine Frage des jeweiligen Underwritings (vgl. Ihlas 2017, Rn. 98). Versicherungsnehmerin ist fast ausnahmslos eine juristische Person, beispielsweise GmbH, AG, SE. Personengesellschaften können auch Versicherungsnehmerin sein. Bei ihnen wird die Kapitalhaftung als Gesellschafter aber nicht vom Versicherungsschutz umfasst. Denn die diesen Gesellschaftstypen immanenten Haftungsprinzipien sollen nicht von der D&O-Versicherung negiert werden. Versichert ist bei Personengesellschaften daher nur die Haftung in dem Umfang, wie die Haftung eines GmbH-Gesellschafters bestünde.

Der Abschluss einer D&O-Versicherung erfolgt durch zur Vertretung berechtigte Personen der Gesellschaft, zum Beispiel durch die Geschäftsführung einer GmbH (vgl. § 35 GmbHG) oder den Vorstand einer AG (vgl. § 78 AktG).

Bei den Unternehmens-D&O-Versicherungen ist das Unternehmen Versicherungsnehmerin und Prämienzahlerin. Die Rechte aus dem Versicherungsvertrag stehen hingegen dem versicherten Unternehmensleiter zu (vgl. § 44 VVG). Es handelt sich um einen Vertrag zugunsten Dritter. Die Prämie, die das Unternehmen zahlt, stellt keine Lohnzuwendung bei den einzelnen Organmitgliedern und damit kein steuerpflichtiges Einkommen dar, solange die D&O-Versicherung das Management als Ganzes absichert, die Versicherung Schäden des Unternehmens abdeckt, Versicherungsansprüche dem Unternehmen zustehen und bei der Prämienkalkulation die Betriebsdaten des Unternehmens Einfluss genommen haben. In diesem Fall ist von einem überwiegend betrieblichen Interesse des Unternehmens am Abschluss der D&O-Versicherung auszugehen (vgl. Finanzministerium Niedersachsen 2002).

Es gibt auch D&O-Versicherungen, die als persönliche D&O-Versicherung aufgebaut sind, das heißt, das Vorstandsmitglied oder der Geschäftsführer kauft die D&O-Versicherung selbst für sich ein. Die betroffene Person wird dann selbst Versicherungsnehmer und Prämienzahler. Dies ist regelmäßig bei D&O-Versicherungen zur Absicherung des gesetzlichen Pflichtselbstbehaltes für Vorstände bzw. des freiwilligen Selbstbehaltes für Aufsichtsratsmitglieder einer deutschen Aktiengesellschaft gemäß der Empfehlung des Deutschen Corporate Governance Kodex (DCGK) in der Fassung 2017 der Fall. Außerhalb dieses Anwendungsfalles könnten sich persönliche D&O-Versicherungen am Markt

allerdings nicht durchsetzen, da sich durch sie nur kleinere Versicherungssummen darstellen lassen und der Versicherungsnehmer und Prämienzahler der Manager selbst ist. Auf diese D&O-Versicherungen soll deswegen nicht weiter eingegangen werden.

24.5.2 Tochtergesellschaften

Die Tochtergesellschaften der Versicherungsnehmerin sind üblicherweise mitversichert. Daraus leitet sich dann auch der Versicherungsschutz für die Manager der Tochtergesellschaften ab. Für die Definition der Tochtergesellschaften greifen die Versicherungsbedingungen üblicherweise auf die Legaldefinition in § 290 Abs. 1 HGB sowie auf § 290 Abs. 2 Nr. 1 bis 3 HGB zurück, so auch die Musterbedingungen des GDV (vgl. AVB-GDV 2019, A-4). In einigen Versicherungsbedingungen wird auch § 290 Abs. 2 Nr. 4 HGB mit einbezogen. Danach sind die Unternehmen Tochtergesellschaften der Versicherungsnehmerin, auf welche die Versicherungsnehmerin direkt oder indirekt einen beherrschenden Einfluss ausüben kann. Beherrschender Einfluss eines Mutterunternehmens besteht nach dem Wortlaut des § 290 Abs. 2 Nr. 1 bis 4 HGB stets:

„wenn

1. ihm bei einem anderen Unternehmen die Mehrheit der Stimmrechte der Gesellschafter zusteht;
2. ihm bei einem anderen Unternehmen das Recht zusteht, die Mehrheit der Mitglieder des die Finanz- und Geschäftspolitik bestimmenden Verwaltungs-, Leitungs- oder Aufsichtsorgans zu bestellen oder abzuberufen, und es gleichzeitig Gesellschafter ist;
3. ihm das Recht zusteht, die Finanz- und Geschäftspolitik auf Grund eines mit einem anderen Unternehmen geschlossenen Beherrschungsvertrages oder auf Grund einer Bestimmung in der Satzung des anderen Unternehmens zu bestimmen, oder
4. es bei wirtschaftlicher Betrachtung die Mehrheit der Risiken und Chancen eines Unternehmens trägt, das zur Erreichung eines eng begrenzten und genau definierten Ziels des Mutterunternehmens dient (Zweckgesellschaft). Neben Unternehmen können Zweckgesellschaften auch sonstige juristische Personen des Privatrechts oder unselbstständige Sondervermögen des Privatrechts sein, ausgenommen Spezial-Sondervermögen im Sinn des § 2 Abs. 3 des Investmentgesetzes oder vergleichbare ausländische Investmentvermögen oder als Sondervermögen aufgelegte offene inländische Spezial-AIF mit festen Anlagebedingungen im Sinn des § 284 des Kapitalanlagegesetzbuchs oder vergleichbare EU-Investmentvermögen oder ausländische Investmentvermögen, die den als Sondervermögen aufgelegten offenen inländischen Spezial-AIF mit festen Anlagebedingungen im Sinn des § 284 des Kapitalanlagegesetzbuchs vergleichbar sind.“

Neu hinzukommende Tochtergesellschaften sind grundsätzlich nach Anzeige durch die Versicherungsnehmerin mitversichert, sofern der Versicherer diese Mitversicherung schriftlich bestätigt (vgl. AVB-GDV 2019, A-4). Bei D&O-Versicherungen für größere

Unternehmensgruppen ist meist eine automatische Mitversicherung neu erworbener oder gegründeter Tochtergesellschaften vereinbart. Die Mitversicherung neuer Tochtergesellschaften erfolgt typischerweise für Ansprüche wegen Pflichtverletzungen nach Closing (rechtliches Inkrafttreten des Unternehmenskaufs), weil der Erwerber normalerweise kein Interesse daran hat, Pflichtverletzungen des alten Managements vor dem Unternehmenskauf in die eigene D&O-Versicherung einzubeziehen. Wenn eine automatische Mitversicherung von Tochtergesellschaften in der D&O-Versicherung gewährt wird, so wird sie regelmäßig nur in bestimmten Grenzen gewährt, das heißt, eine automatische Mitversicherung erfolgt nur innerhalb definierter Umsatz- oder Bilanzsummengrenzen. Außerdem sind bestimmte Risiken, wie zum Beispiel US-Tochtergesellschaften oder Finanzinstitute, regelmäßig von einer automatischen Mitversicherung ausgenommen.

Ehemalige Tochtergesellschaften bleiben meist unbefristet dergestalt in der D&O-Versicherung mitversichert, dass eine Inanspruchnahme wegen einer Pflichtverletzung versichert bleibt, wenn die Gesellschaft zum Zeitpunkt der Pflichtverletzung als Tochtergesellschaft mitversichert war.

Einrichtungen der betrieblichen Altersversorgung sind weltweit meist rechtlich selbstständig und vom Sponsor-Konzern unabhängig, sodass sie keine Tochtergesellschaften im Sinne der oben genannten Definition sind. Der Versicherungsmarkt bietet für sie sogenannte Pension-Trust-Liability-Versicherungen an, die auf die Besonderheiten der baV-Einrichtungen abgestimmt sind. Sofern man sie dennoch mit in den D&O-Versicherungsvertrag einbeziehen möchte, müssen sie ausdrücklich namentlich erfasst werden. Im Falle ihrer Einbeziehung wird der Versicherungsschutz grundsätzlich mit einem Berufshaftpflichtausschluss versehen. Dieser begrenzt über einen generellen Ausschluss mit Wiedereinschluss den Versicherungsschutz auf Organisationspflichtverletzungen. Risiken der Manager aus der operativen Tätigkeit bleiben im Regelfall vom Versicherungsschutz ausgenommen.

24.5.3 Versicherte Personen

Versichert sind die Organmitglieder und zwar die gegenwärtigen oder ehemaligen Mitglieder des Aufsichtsrates, des Vorstandes oder der Geschäftsführung des Versicherungsnehmers oder einer Tochtergesellschaft (vgl. AVB-GDV 2019, A-1). Durch die am Markt verwendeten Bedingungen sind auch zukünftige Unternehmensleiter mitversichert (vgl. Ihlas 2017, Rn. 154 ff.). Über die Organmitglieder hinaus, die stets von der Versicherung erfasst sind, wird der Kreis der versicherten Personen regelmäßig auf verschiedene andere Manager unterhalb der Organebene erweitert. Dabei werden in der Versicherungspraxis auch Personen versichert, die ein deutlich geringeres Haftungsrisiko als Organmitglieder haben. So werden unterhalb der Organebenen beispielsweise leitende Angestellte erfasst, für die in Deutschland jedoch schon die Haftungsmilderungen für Arbeitnehmer gelten. In vielen D&O-Versicherungen ist der Kreis der versicherten Personen zudem auf Compliance Officer oder besondere vom Gesetzgeber oder durch Industriestandards vorgesehene

Beauftragte zur Sicherstellung der Compliance erweitert, wie zum Beispiel auf Datenschutz-, Geldwäsche-, Arbeitsschutz- oder Sicherheitsbeauftragte, Chief Legal Officer, Risk Manager; auf „Shadow Directors“, „Approved Persons“ (UK und Irland) und Mitglieder der „Organo di Vigilanza“ und „Organo collegiale di Vigilanza (Italien)“.

Eine namentliche Nennung der versicherten Personen erfolgt ansonsten nicht. Es werden alle Personen der versicherten Gruppen pauschal versichert.

Vom Versicherungsschutz umfasst sind regelmäßig auch die Organmitglieder und anderen versicherten Manager in den Tochtergesellschaften der Versicherungsnehmerin. Der Kreis der versicherten Personen leitet sich immer von dem Unternehmen ab, das sie zum Organ bestellt hat oder bei dem sie angestellt sind. Das heißt, zunächst muss die Gesellschaft zu den mitversicherten Gesellschaften gehören, und daran anschließend kommt es darauf an, ob die Person unter die Definition der versicherten Personen fällt.

24.6 Zeitlicher Umfang des Versicherungsschutzes

24.6.1 Claims-made-Prinzip

Versicherungsschutz besteht grundsätzlich nur für Versicherungsfälle, die während der Dauer der Versicherung eintreten. In der D&O-Versicherung tritt der Versicherungsfall typischerweise mit der erstmaligen schriftlichen Geltendmachung eines Haftpflichtanspruchs gegen eine versicherte Person ein. Dieses wird auch als Claims-made- oder Anspruchserhebungsprinzip bezeichnet.

Nur wenige D&O-Versicherungen liegen als Versicherungsfall das Verstoßprinzip zugrunde, bei dem es darauf ankommt, wann die Pflichtverletzung (also das verursachende Geschehen bzw. das haftungsauslösende Verhalten) begangen worden ist. Gilt das Verstoßprinzip, muss die Pflichtverletzung während der Vertragslaufzeit erfolgt sein, unabhängig vom Zeitpunkt der Inanspruchnahme. Die Absicherung durch den Versicherer steht also unbegrenzt auch nach dem Ablauf der Police zur Verfügung (sogenannte Nachhaftung) und birgt damit für den Versicherer eine Spätschadenproblematik (vgl. Ihlas 2017, Rn. 241). Das ist bei der D&O-Versicherung typischerweise anders. Es gibt nur vereinzelt Versicherer, die D&O-Versicherungen auf Basis des Verstoßprinzips anbieten. Einige dieser D&O-Versicherungen sind nicht als Unternehmensdeckungen konzipiert, sondern als persönliche D&O-Versicherung, die der Manager privat einkauft. Mit diesen Deckungskonzepten stößt man allerdings schnell auf Probleme bei den Versicherungssummenkapazitäten.

Üblich sind am Markt Unternehmensdeckungen nach dem Claims-made-Prinzip. Beim Claims-made-Prinzip kommt es zunächst nicht darauf an, wann die Pflichtverletzung begangen worden ist. Es kommt nur auf den Zeitpunkt an, an dem eine versicherte Person erstmalig schriftlich auf Schadensersatz in Anspruch genommen wird. Dadurch ist der Eintritt des Versicherungsfalls zeitlich klar. Zudem ist der Eintritt des Versicherungsfalls einfacher zu beweisen.

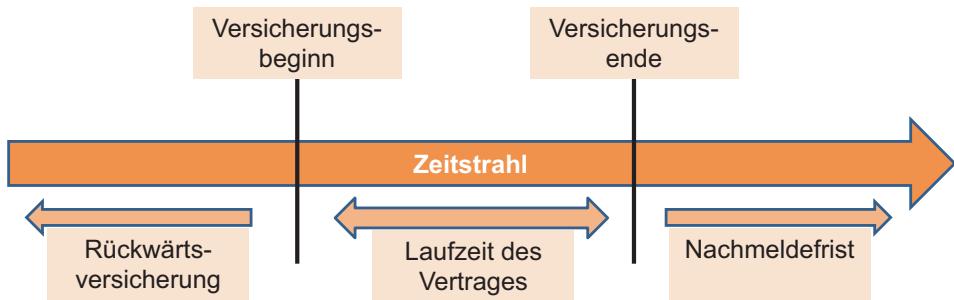


Abb. 24.1 Claims-made-Prinzip. (Quelle: eigene Darstellung in Anlehnung an Held 2006, 33. Kapitel, Rn. 23)

Die D&O-Versicherung gilt wie andere Versicherungen der Haftpflicht-Sparte als „long tail business“ für die Versicherer. Dies bedeutet, dass zwischen der begangenen Pflichtverletzung und der erstmaligen Anspruchserhebung mehrere Jahre liegen können. Ferner benötigt eine Abwicklung des Versicherungsfalls nach Anspruchserhebung regelmäßig bis zu sieben Jahren (vgl. Ihlas 2017, Rn. 239).

Abb. 24.1 veranschaulicht das Anspruchserhebungsprinzip/Claims-made-Prinzip.

24.6.2 Rückwärtsversicherung

Für die D&O-Versicherung mit Claims-made-Prinzip kommt es nicht auf den Zeitpunkt des Verstoßes an. Der Anspruch muss lediglich während der Vertragslaufzeit erhoben werden (vgl. AVB-GDV 2019, A-5.1). Der Versicherungsschutz umfasst auch Inanspruchnahmen wegen Pflichtverletzungen, die vor Beginn des Versicherungsvertrages begangen wurden. Pflichtverletzungen, welche die versicherte Person bei Vertragsabschluss kannte, sind nicht in den Versicherungsschutz einbezogen. Als bekannt gelten Pflichtverletzungen, wenn die versicherte Person oder die Versicherungsnehmerin eine Pflichtverletzung für möglich hält oder jemand eine mögliche Pflichtverletzung behauptet hat (vgl. AVB-GDV 2019, A-5.2).

Die Rückwärtsdeckung sorgt für eine Zuordnung eines Haftpflichtanspruchs zur aktuellen Police (vgl. Schmitt, S. 129). Das ist beim erstmaligen Abschluss einer D&O-Versicherung ein erheblicher Vorteil des Claims-made-Prinzips gegenüber dem Verstoßprinzip, weil durch das Claims-made-Prinzip auch Pflichtverletzungen aus der Vergangenheit erfasst werden. Deckungslücken können sowohl beim erstmaligen Abschluss einer D&O-Versicherung als auch bei einem Versichererwechsel auftreten, wenn eine Rückwärtsversicherung nicht greift oder nicht vereinbart wird.

24.6.3 Nachmeldefrist

Werden Schadenersatzansprüche erst nach Ablauf des Versicherungsvertrages erhoben, die auf eine Pflichtverletzung während der Versicherungszeit zurückzuführen sind, sind diese nach dem Claims-made-Prinzip ungedeckt, wenn keine abweichende Regelung vereinbart ist. Im deutschsprachigen Raum ist es üblich, dass die Versicherer eine lange Nachmeldefrist und somit eine Nachhaftung der Versicherungspolice einräumen. Hierbei sind Ansprüche, die auf Pflichtverletzungen innerhalb der Vertragslaufzeit zurückzuführen sind, auch nach Ablauf des Vertrages während der bestimmten Frist mitversichert (vgl. AVB-GDV 2019, A-5.3). Ist die Nachmeldefrist abgelaufen, besteht kein Versicherungsschutz über die beendete D&O-Versicherung. In USA oder am Londoner Versicherungsmarkt sind deutlich kürzere Nachmeldefristen als in Deutschland üblich, so dass die Versicherer das Risiko im Falle einer Vertragsbeendigung nur noch für kurze Zeit oder gar nicht mehr tragen. Das ist für die versicherten Personen ein hohes Risiko, denn eine Inanspruchnahme kann auch Jahre nach der Pflichtverletzung erfolgen. Grundsätzlich gilt, je länger die Nachmeldefrist, desto besser. Innenansprüche einer GmbH gegen ihre Geschäftsführer sowie einer Aktiengesellschaft gegen ihre Vorstände verjährten in fünf Jahren ab ihrer Entstehung (vgl. § 43 Abs. 4 GmbHG, § 93 Abs. 6 AktG). Bei börsennotierten Aktiengesellschaften verlängert sich die Verjährung auf zehn Jahre, wenn die Gesellschaft zum Zeitpunkt der Pflichtverletzung börsennotiert war (vgl. § 93 Abs. 6 AktG).

Der deutsche Versicherungsmarkt bietet meist eine unverfallbare und prämiennetrale kurze Nachmeldefrist mit einer Verlängerungsmöglichkeit gegen Mehrprämie an. Dabei sind die Zukaufoptionen üblicherweise fest vereinbart, wobei sich der Zuschlagssatz nach der letzten Jahresprämie bestimmt. Dem Versicherungsschutz während der Nachmeldefrist liegen die Vertragsbestimmungen der letzten Versicherungsperiode zu Grunde. Die Versicherungssumme der letzten Versicherungsperiode gilt weiterhin. Versicherungsfälle während der Nachmeldefrist werden ihr zugeordnet (vgl. AVB-GDV 2019, A-5.4).

24.6.4 Meldung von Umständen

Zeigen sich Umstände, die zu einer Inanspruchnahme einer versicherten Person und mit hin zu einem Versicherungsfall führen könnten, können sie dem Versicherer angezeigt werden. Kommt es später zu einer Inanspruchnahme, gilt der Zeitpunkt der Umstandsmeldung als Zeitpunkt der Inanspruchnahme. Die Umstandsmeldung schützt die versicherte Person davor, dass der Versicherer den Vertrag beendet oder aus einem Versicherungskonsortium aussteigt, wenn sich eine Inanspruchnahme abzeichnet. Eine wirksame Umstandsmeldung sichert die Position der versicherten Person. Sie ist ein unverzichtbares Element des Claims-made-Prinzips (vgl. Ihlas 2017, Rn. 253). An eine wirksame Umstandsmeldung dürfen aus Sicht der versicherten Person daher nicht allzu hohe Anforderungen gestellt werden. Müssen konkrete Angaben zu Pflichtverletzungen gemacht werden oder die Inanspruchnahme einer versicherten Person hinreichend wahrscheinlich sein, damit sie

wirksam ist, gelingt eine Umstandsmeldung oftmals nicht. Das ist besonders problematisch, wenn eine D&O-Versicherung beendet wird oder es zu Wechseln im Versicherungskonsortium kommt. Für eine neue D&O-Versicherung gilt regelmäßig ein umfassender Ausschluss bekannter Umstände. Gelingt eine Umstandsmeldung nicht oder nicht vollständig, läuft die versicherte Person Gefahr, dass sämtliche Ansprüche im Zusammenhang mit dem bekannten Umstand von einem zukünftigen Versicherungsschutz ausgeschlossen sind, ohne dass die versicherte Person in der alten D&O-Versicherung Deckung erhält.

24.7 Sachlicher Umfang des Versicherungsschutzes

Der D&O-Versicherungsmarkt bietet ein breites Spektrum an Ausgestaltungsmöglichkeiten des Versicherungsschutzes an, um den unterschiedlichen Bedürfnissen von Unternehmen gerecht zu werden. Schätzungen besagen, dass die führenden Versicherungsunternehmen im Bereich der D&O-Versicherung über 500 Klauseln zur individuellen Vertragsgestaltung auf Abruf bereithalten (vgl. Halm et al. 2015, Kap. 33, Rn. 19). Nachfolgend wird auf Grundlage der AVB D&O des GDV ein Überblick über den sachlichen Umfang des Versicherungsschutzes einer D&O-Police gegeben:

24.7.1 Abwehr und Freistellung

Die D&O-Versicherung enthält zwei grundlegende Versicherungsschutzfunktionen:

Zum einen umfasst die D&O-Versicherung die Prüfung der Haftpflichtfrage und die Abwehr unberechtigter Ansprüche. Zum anderen wird die versicherte Person von berechtigten Ansprüchen durch den Versicherer freigestellt (vgl. AVB-GDV 2019, A-6.1). Die D&O-Versicherung bietet Rechtsschutz und Befreiung von einer Verbindlichkeit (vgl. Ihlas 2017, Rn. 369). Der Versicherer stellt den Versicherten von einem Anspruch frei, indem er direkt an den geschädigten Dritten zahlt oder den Anspruch in sonstiger Weise befriedigt.

Der Versicherer hat das Recht, Prozesse im Namen der versicherten Person zu führen (vgl. AVB-GDV 2019, A-6.2).

24.7.2 Versicherungssummen und Kosten

Die Versicherungssumme begrenzt die Leistungspflicht des Versicherers. Sie ist die Höchstersatzleistung des Versicherers. Meist ist sie einfach maximiert, das heißt, der Versicherer zahlt je Versicherungsfall und zugleich für alle Versicherungsfälle maximal die Versicherungssumme. Abwehrkosten, sowohl gerichtlich als auch außergerichtlich, werden auf diese Versicherungssumme angerechnet (vgl. AVB-GDV 2019, A-6.4). Eine Defi-

nition der Kosten ist nur selten gegeben (vgl. Ihlas 2017, Rn. 513). Die Musterbedingungen des GDV führen Anwalts-, Sachverständigen-, Zeugen- und Gerichtskosten auf, wobei diese Aufzählung nicht abschließend ist. Unter Abwehrkosten fallen unter anderem auch: Steuerberatungskosten, Konfliktmanagementkosten, Kosten forensischer Dienstleistungen, Kosten der Zeugenvernehmung, Reisekosten, Schadenminderungskosten, Schadenregulierungskosten sowie Kosten der Stellung einer Sicherheitsleistung zur Abwehr einer Zwangsvollstreckung (vgl. Ihlas 2017, Rn. 514).

Die richtige Versicherungssumme zu wählen, ist nicht einfach. Wie bei jeder Haftpflichtversicherung muss abgeschätzt werden, welche Ansprüche entstehen und in welcher Höhe diese ausfallen können. Im Zweifel empfiehlt es sich, die Versicherungssumme etwas großzügiger zu bemessen. Reicht die Versicherungssumme nicht aus, muss der in Anspruch genommene Manager ggf. mit seinem Privatvermögen eintreten. Der Einfachheit halber wird bei kleineren und mittleren Unternehmen üblicherweise eine Versicherungssumme von zehn Prozent der Bilanzsumme angesetzt (vgl. Ihlas 2017, Rn. 508). Diese Quote ist bei Großunternehmen nicht anwendbar. Versicherungssummen von über 500 Millionen Euro sind aktuell am weltweiten Versicherungsmarkt kaum darstellbar, so dass multinationale Großunternehmen in der Regel nur die Summe einkaufen, die unter Berücksichtigung der Marktgegebenheiten sinnvoll ist.

Aufgrund des Claims-made-Prinzips ist die Versicherungssumme im Jahr der Anspruchserhebung und nicht die Versicherungssumme im Jahr des Verstoßes relevant. Das bietet den Vorteil, dass die Versicherungssummeschneller an die allgemeine Entwicklung des Haftungsumfeldes angepasst werden kann. Möchte eine Versicherungsnehmerin im Laufe der Jahre die Versicherungssumme der D&O-Versicherung erhöhen, so muss sie regelmäßig gegenüber dem Versicherer eine Erklärung abgeben, dass keine Pflichtverletzungen bekannt sind, die zu Ansprüchen führen können, die die vorher vereinbarte Versicherungssumme übersteigen (vgl. Ihlas 2017, Rn. 507). So soll verhindert werden, dass kurz vor einer Inanspruchnahme die Versicherungssumme erhöht wird.

Für kleinere und mittlere Unternehmen besteht die Möglichkeit, eine mehrfach maximierte Versicherungssumme und eine Klausel zur Wiederauffüllung der Versicherungssumme zu vereinbaren (vgl. Ihlas 2017, Rn. 510 f.). Die Zusatzprämien für diese Klauseln sind von der Versicherungsnehmerin zu leisten und werden von Versicherer zu Versicherer unterschiedlich kalkuliert (vgl. Ihlas 2017, Rn. 511 f.).

24.7.3 Selbstbehalt

Ein Selbstbehalt für die versicherten Manager ist in der D&O-Versicherung nicht üblich, auch wenn die Musterbedingungen des GDV einen generellen Selbstbehalt vorsehen (vgl. AVB-GDV 2019, A-6.5). Eine Ausnahme bilden Organmitglieder von Aktiengesellschaften. Für den Vorstand einer Aktiengesellschaft ist ein Selbstbehalt gesetzlich vorgeschrieben. Gemäß § 93 Abs. 2 S. 3 AktG ist ein Selbstbehalt in Höhe von zehn Prozent des eingetretenen Schadens bis zu einer Höhe des 1,5-fachen der Jahresvergütung zu vereinbaren.

Die Bemessung des Selbstbehaltes erfolgt anhand der Vergütung im Jahr des Pflichtverstoßes und bezieht sich nur auf die Schaden-, und nicht auf die Abwehrkosten (vgl. Ihlas 2017, Rn. 492 ff.). Der Deutsche Corporate Governance Kodex (DCGK) 2017 empfiehlt in Ziffer 3.8, auch für die Aufsichtsratsmitglieder einer börsennotierten Aktiengesellschaft einen entsprechenden Selbstbehalt zu vereinbaren. Hieran halten sich viel der dem Kodex entsprechenden Unternehmen. Der Entwurf des neuen DCGK 2019 sieht diese Empfehlung nicht mehr vor. Nach Inkrafttreten des neuen DCGK 2019 kann es gleichwohl notwendig sein, einen Selbstbehalt für die Aufsichtsratsmitglieder zunächst fortzuführen, wenn die Aktiengesellschaft bislang erklärt hat, den Empfehlungen des DCGK 2017 zu entsprechen.

Für den Geschäftsführer einer GmbH gibt es keine gesetzliche Vorschrift, die einen Selbstbehalt vorschreibt (vgl. Graf von Westphalen 2016, Rn. 161).

Die von einem Selbstbehalt betroffenen Manager können ihn durch eine D&O-Selbstbehalt-Versicherung absichern.

Der gesetzliche Pflichtselbstbehalt ist ein deutscher Sonderweg. Der Gesetzgeber hätte den Pflichtselbstbehalt nicht einführen müssen, um das Verantwortungsbewusstseins der Manager zu stärken. Eine Inanspruchnahme stellt für jeden Manager eine Ausnahmesituation dar, die sehr unangenehm und belastend ist. Allein die finanzielle Absicherung durch eine D&O-Versicherung kann dies nicht kompensieren, auch wenn der Manager sich an einer Entschädigungsleistung nicht beteiligen muss.

Bieten D&O-Versicherungen (wie üblich) Versicherungsschutz auch für den Fall, dass das Unternehmen einen versicherten Manager von einem Haftungsanspruch eines Dritten freistellt, so sehen die Klauseln für das Unternehmen einen Selbstbehalt vor. In diesem Fall befreit das Unternehmen den Manager von der Inanspruchnahme.

Für den Fall, dass Versicherungsschutz für den Fall einer Inanspruchnahme eines (börsennotierten) Unternehmens wegen der Verletzung einer Wertpapierhandelsrechtlichen Regelung vereinbart ist, sind ebenfalls Selbstbehalte üblich; meist als Eigenbehalt, das heißt, der Versicherer übernimmt bis zum Erreichen einer Eigenbehaltsgrenze auch nicht die Kosten für die Abwehr eines unberechtigten Anspruchs.

24.7.4 Erweiterungen des Versicherungsschutzes

Im Wettstreit um die Gunst der Kunden wurden von Jahr zu Jahr neue Deckungserweiterungen entwickelt. Mittlerweile bietet der Versicherungsmarkt eine Vielzahl an Deckungserweiterungen. Nicht alle am Markt angebotenen Deckungserweiterungen lassen einen nennenswerten Mehrwert für die Versicherten erkennen. Einige Deckungserweiterungen sollen im Folgenden exemplarisch aufgegriffen werden. Zumeist ist eine Deckungserweiterung sublimiert, das heißt, es besteht eine summenmäßige Limitierung innerhalb der Versicherungssumme der D&O-Versicherung, welche die Höchstersatzleistung des Versicherers im Schadenfall für die spezifische Deckungserweiterung begrenzt.

24.7.4.1 Aktiver Rechtsschutz (negative Feststellungsklage)

Der Versicherungsmarkt bietet üblicherweise in den Standard D&O-Versicherungsbedingungen eine Erweiterung des Versicherungsschutzes für die Kosten einer negativen Feststellungsklage für den Fall, dass einer versicherten Person schriftlich vorgeworfen wird, eine Pflichtverletzung begangen zu haben, ohne dass bereits ein Haftpflichtanspruch geltend gemacht ist. Durch eine negative Feststellungsklage kann gerichtlich festgestellt werden, dass ein Rechtsverhältnis nicht besteht, obwohl dies ein Dritter behauptet. Wird eine Pflichtverletzung behauptet, kann der versicherte Manager selbst die Initiative ergreifen und gerichtlich feststellen lassen, dass er die ihm vorgeworfene Pflichtverletzung nicht begangen hat. Die Kosten hierfür trägt der D&O-Versicherer.

24.7.4.2 Ungerechtfertigte Bereicherung

In vielen D&O-Versicherungen findet sich eine Deckungserweiterung für den Fall einer Inanspruchnahme einer versicherten Person wegen ungerechtfertigter Bereicherung (vgl. §§ 812 ff. BGB). Der Versicherer trägt üblicherweise nur die Kosten zur Abwehr eines solchen Anspruchs, nicht jedoch die Rückzahlung des unberechtigt Erlangten, wenn der Anspruch berechtigt ist. Zudem muss der versicherte Manager dem Versicherer meist die Abwehrkosten ersetzen, wenn eine ungerechtfertigte Bereicherung tatsächlich vorliegt.

24.7.4.3 Strafrechtsschutz

Versicherungsschutz für Verteidigungskosten in einem Straf- oder Ordnungswidrigkeitsverfahren, einem standesrechtlichen Verfahren, einem verwaltungsrechtlichen Verfahren oder einem anderen behördlichen Verfahren kann zudem für den Fall vereinbart werden, dass dem Verfahren ein Ereignis zu Grunde liegt, das einen unter den Versicherungsschutz fallenden Haftpflichtanspruch zur Folge haben kann. Der Versicherungsschutz wird für diese Fälle auf die Erstattung von Kosten für die Verteidigung (Rechtsanwaltskosten) der versicherten Personen erweitert. Es werden meist die gebührenordnungsmäßigen, ggf. die mit dem Versicherer besonders vereinbarten höheren Kosten des Verteidigers erstattet.

Diese Deckungserweiterung gleicht einen entscheidenden Nachteil der gesetzlichen Regelung in § 101 VVG aus. Nach § 101 VVG muss der Versicherer zwar die gerichtlichen und außergerichtlichen Kosten in einem Strafverfahren tragen, das wegen einer Tat eingeleitet wurde, welche die Verantwortlichkeit des Versicherungsnehmers gegenüber einem Dritten zur Folge haben könnte. Das gilt allerdings nur dann, wenn der D&O-Versicherer die Weisung erteilt hat, sich verteidigen zu lassen und nur für die auf Weisung des Versicherers aufgewendeten Kosten. Bei der Deckungserweiterung für Strafrechtsschutz muss der versicherte Manager lediglich darlegen und ggf. beweisen, dass ein Haftpflichtanspruch droht. Ist das der Fall, muss der Versicherer die Kosten der Verteidigung tragen. Auf eine Weisung des Versicherers kommt es nicht an.

Eine eigenständige Strafrechtsschutzversicherung kann die oben beschriebene Deckungserweiterung in der D&O-Versicherung allerdings nicht ersetzen. Der Deckungsumfang von Strafrechtsschutzversicherungen ist deutlich weiter. So ist zum Beispiel bei einer

Deckung unter einer Strafrechtsschutzversicherung nicht relevant, ob in der Folge ein Haftpflichtanspruch droht.

24.7.4.4 Gehaltsfortzahlung oder Existenzsicherung durch Darlehen

Mit behaupteten Haftpflichtansprüchen des Unternehmens gegen versicherte Personen wird bei Innenansprüchen häufig gegen Vergütungsansprüche der versicherten Person aufgerechnet. Der Versicherungsmarkt bietet eine Deckungserweiterung für eine „Gehaltsfortzahlung“ oder ein Darlehen als Ersatz für den Vergütungsanspruch. Der Versicherer zahlt für einen bestimmten Zeitraum eine Art Einkommen. Die Ausgestaltung dieser Deckungserweiterung ist unterschiedlich. Teilweise wird eine „Gehaltsfortzahlung“ durch den Versicherer geboten, teilweise vergibt der Versicherer ein sicherungsfreies Darlehen.

24.7.4.5 PR-Berater und Krisenberater

Insbesondere für Manager, die in der Öffentlichkeit stehen, kann es in Haftungsfällen sinnvoll sein, einen PR- oder Krisen-Berater zu Rate zu ziehen. Die Presseabteilungen von Unternehmen, sofern vorhanden, sind nicht auf die Bewältigung einer persönlichen Haftungskrise eines Managers spezialisiert und im Falle eines Innenanspruchs besteht auch gar kein Interesse des Unternehmens daran, die versicherte Person zu unterstützen. Die D&O-Versicherung lässt sich um einen Kostenbaustein erweitern, wonach PR- und Krisenberater-Kosten übernommen werden. Die Beauftragung ist jedoch oft mit dem Versicherer abzustimmen

24.7.4.6 Psychologische Betreuung

Einige D&O-Versicherungen sehen zudem eine Deckungserweiterung für psychologische Beratung vor. Der D&O-Versicherer übernimmt die angemessenen Kosten einer psychologischen Betreuung des Managers sowie des Ehe-/Lebenspartners mit dem Ziel der Stressbewältigung durch einen anerkannten Psychologen oder Psychiater. Das mag seltsam erscheinen, weil „gestandene Manager“ in der D&O-Versicherung versichert werden, die an Stress gewohnt und dementsprechend stressresistent sein sollten. Der Stress einer persönlichen Inanspruchnahme des Managers sollte aber nicht unterschätzt werden. Geht es doch um Höchstpersönliches und darüber hinaus auch um das Privatvermögen des Managers, das er möglicherweise über viele Jahre oder Jahrzehnte aufgebaut hat.

24.7.4.7 Kontinuitätsgarantie

Für kleinere und mittlere Unternehmen wird teilweise auch eine Kontinuitätsgarantie geboten. Der Versicherer verpflichtet sich in den Vertragsbedingungen dazu, etwaige zukünftige Bedingungseinschränkungen nicht auf Pflichtverletzungen anzuwenden, die vor der Wirksamkeit der Bedingungseinschränkungen eingetreten sind. Das heißt, der alte Bedingungsumfang bleibt für Ansprüche wegen dieser Pflichtverletzungen erhalten. Diese Deckungserweiterung ist allerdings systematisch nicht zwingend, da sie im Widerspruch zum Claims-made-Prinzip steht.

24.7.5 Abgrenzung zu anderen Versicherungen

In der Praxis hat die Abgrenzung zwischen der D&O-Versicherung und weiteren Versicherungsprodukten eine zunehmende Relevanz. Abgrenzungsprobleme treten insbesondere mit einer Cyber-Versicherung, aber auch mit einer IPO-Deckung (Prospekthaftungsversicherung), Strafrechtsschutzversicherung, PTL-Versicherung (Pension Trust Liability-Versicherung), Berufshaftpflichtversicherung (hier: Vermögensschaden-Haftpflichtversicherung), IT-Haftpflichtversicherung oder auch mit der Allgemeinen Haftpflichtversicherung und Umwelthaftpflichtversicherung auf (vgl. Finkel und Seitz 2016, Rn 91), weil diese Versicherungen Versicherungsschutz für bestimmte Inanspruchnahmen wegen Vermögensschäden bieten und die Manager dort oftmals mitversichert sind. Bei der Abgrenzung der D&O-Versicherung von anderen Versicherungen ist insbesondere auf Subsidiaritätsregelungen und Risikoausschlüsse zu achten und zu prüfen, wer aufgrund welcher Handlung in Anspruch genommen wird (vgl. Finkel und Seitz 2016). Die D&O-Versicherung kann andere Haftpflichtversicherungen nicht ersetzen. Alle vorgenannten Versicherungslösungen verfolgen einen eigenen Ansatz. Gleichwohl kann es zu Überschneidungen mit der D&O-Versicherung kommen und ungewollt eine Mehrfachversicherung entstehen.

Bei der Gestaltung sollte das Rangverhältnis der Deckungen geregelt und sichergestellt werden, dass der Versicherungsschutz einer Police zugewiesen wird und nicht gänzlich entfällt, weil der Versicherungsschutz weder in der einen noch in der anderen Police erhalten bleibt. Die Regelungen in den Musterbedingungen des GDV (vgl. B-4-1.1 und AVB-GDV 2019, A-7) sind sehr weitgehend. Aus Sicht der versicherten Personen empfiehlt sich eine Überprüfung und eine Streichung von Ausschlüssen zugunsten von Subsidiaritätsregelungen, sodass der Versicherungsschutz in der D&O-Versicherung nachrangig zu einem anderweitigen Versicherungsschutz erhalten bleibt.

Subsidiaritätsregelungen in verschiedenen Verträgen müssen aufeinander abgestimmt werden, damit nicht in allen Verträgen Regelungen enthalten sind, wonach sie nur nachrangig leisten, wenn ein Versicherungsfall auch unter einer anderen Versicherung versichert ist, sodass am Ende kein Versicherer zu leisten bereit ist.

Dies gilt auch für anderweitige D&O-Versicherungen. Werden beispielsweise Unternehmen gekauft, so sollten Regelungen zur Abgrenzung zwischen den betroffenen D&O-Deckungen getroffen werden.

24.8 Örtlicher Geltungsbereich

Die Musterbedingungen des GDV schließen Ansprüche vom Versicherungsschutz aus, die außerhalb der EU gerichtlich verfolgt oder nach außereuropäischen (EU) Rechtsordnungen geltend gemacht werden sowie Schäden wegen der Verletzung nichteuropäischen (EU) Rechts (vgl. AVB-GDV 2019, A-7.5). So sind Haftpflichtansprüche vom Versicherungsschutz ausgeschlossen, welche vor Gerichten außerhalb der EU oder nach dem Recht von Staaten, die nicht der EU angehören, geltend gemacht werden (dies gilt auch im Falle

der Vollstreckung von Urteilen, die außerhalb der EU gefällt wurden) sowie wegen Schäden aus der Verletzung oder Nichtbeachtung des Rechts von Staaten, die nicht der EU angehören. In marktüblichen Policen wird eine EU- oder weltweite Deckung geboten. Lediglich für die USA sind aufgrund des höheren Risikos generell Einschränkungen üblich (vgl. Ihlas 2017, Rn. 575 f.). Bei D&O-Versicherungen für kleine Unternehmen kann der Geltungsbereich auf Deutschland eingeschränkt sein, bei Bedarf aber regelmäßig erweitert werden. Großunternehmen sind meist auch in den USA aktiv oder haben dort Tochtergesellschaften, so dass der Geltungsbereich entsprechend ausgestaltet sein sollte.

Wenn die Versicherungsnehmerin Tochtergesellschaften im Ausland hat, sollten für diese im Rahmen eines sogenannten internationalen Versicherungsprogramms ggf. Lokalpolicen vereinbart werden. Das heißt, es sollten vor Ort D&O-Versicherungen eingekauft werden, möglichst bei dem Versicherer bzw. Versicherungskonzern, bei dem die Versicherungsnehmerin die D&O-Versicherung abgeschlossen hat. Notwendig ist dies in Ländern, in denen ein deutscher oder europäischer Versicherer keinen Versicherungsschutz bieten darf. Der Abschluss lokaler Policen kann sich aber auch empfehlen, um ggf. lokalen Besonderheiten abzudecken. Insbesondere in den USA sollte eine lokale D&O-Versicherung abgeschlossen werden. Ohne ihren Nachweis kann es dort sonst schwierig werden, Manager für das Unternehmen zu gewinnen.

Die D&O-Versicherung der deutschen Muttergesellschaft wird bei einem internationalen Programm um eine sogenannte Konditionen- und eine Summandifferenzdeckung erweitert. Diese Deckungserweiterungen stellen den Inhalt und Umfang der D&O-Versicherung der deutschen Muttergesellschaft auch für die Tochtergesellschaften mit einer Lokalpolice sicher. Diese sogenannte Masterdeckung erfüllt (im Rahmen der eigenen D&O-Versicherungsbedingungen) geringere Standards im lokalen Versicherungsschutz, sowohl dem Inhalt als auch in Bezug auf die Höhe der Versicherungssumme.

24.9 Ausschlüsse

Ausschlüsse dienen dem Versicherer dazu, das versicherte Risiko einzuschränken, und somit letztlich der Kalkulation des Risikos und der Prämie. Besonders im Falle der D&O-Versicherung sollen Risikoausschlüsse ferner der Spartentrennung dienen, da sonst Vermögensschäden, die im Deckungsumfang anderer Versicherungen enthalten sind, im Rahmen der D&O-Versicherung geltend gemacht werden könnten (vgl. Finkel und Seitz 2016, S. 482). Der Wert einer D&O-Police bestimmt sich unter anderem auch durch die Ausschlüsse.

Der vom GDV erstellte Ausschlusskatalog unter A-7 AVB D&O ist sehr breit aufgestellt und stellt eher ein Baukastensystem für die Ausschlusskataloge der Versicherer dar. Im Folgenden soll auf nur wenige Ausschlüsse eingegangen werden:

24.9.1 Vorsatz

Der Ausschluss vorsätzlicher bzw. wissentlicher Pflichtverletzungen ist der bedeutendste Ausschluss in der D&O-Versicherung.

Bereits durch § 103 VVG ergibt sich die Leistungsfreiheit des Versicherers, wenn der Versicherungsnehmer vorsätzlich und widerrechtlich einen Schaden bei einem Dritten herbeiführt. Nicht ausgeschlossen sind grob fahrlässig herbeigeführte Schäden (vgl. Finkel und Seitz 2016, S. 485).

Die Musterbedingungen des GDV erweitern die gesetzliche Regelung um den Ausschluss der wissentlichen Pflichtverletzung. Unter wissentlicher Pflichtverletzung versteht man das wissentliche Abweichen von Gesetz, Vorschrift, Beschluss, Vollmacht oder Weisung (vgl. A-7.1 AVB D&O). Den Versicherungsschutz verliert, wenn eine Pflicht bewusst ist und er dennoch bewusst von dieser Pflicht abweicht (Pflichtverletzungsbewusstsein) (vgl. Finkel und Seitz 2016, S. 488).

Statt einer „wissentlichen Pflichtverletzung“ schließen viele Versicherer vorsätzliche Pflichtverletzungen vom Versicherungsschutz aus. Bei vorsätzlichen Pflichtverletzungen genügt eine Inkaufnahme der Pflichtverletzung (Eventualvorsatz), unabhängig vom Wissen über diese (vgl. Finkel und Seitz 2016, S. 489 f.). Daraus ergibt sich, dass für die versicherte Person die Formulierung des Ausschlusses einer wissentlichen Pflichtverletzung besser ist, da hier eine Inkaufnahme nicht genügt, sondern ein positives Wissen vorliegen muss (vgl. Finkel und Seitz 2016, S. 490). Wenn in D&O-Versicherungen eine vorsätzliche Pflichtverletzung ausgeschlossen ist, ist der Ausschluss meist eingeschränkt, das heißt, bedingt vorsätzliche Pflichtverletzungen bleiben mitversichert. Beim bedingten Vorsatz (dolus eventalis) wird eine Pflichtverletzung billigend in Kauf genommen.

Der Versicherungsschutz wird in den allermeisten D&O-Versicherungen zunächst gewährt, wenn streitig ist, ob eine vorsätzliche bzw. wissentliche Pflichtverletzung vorliegt. Dieses ist äußerst wichtig, um Deckungsstreitigkeiten über die Übernahme der Abwehrkosten durch den Versicherer zu vermeiden. Der D&O-Versicherer zahlt die Abwehrkosten, solange der Vorsatz bzw. die Wissentlichkeit nicht rechtskräftig, zum Beispiel durch Urteil, festgestellt ist. Erfolgt eine solche Feststellung, entfällt der Versicherungsschutz rückwirkend und dem Versicherer sind die bis dahin von ihm aufgewandten Kosten zurückzu erstatten.

Zusätzlich bieten einige D&O-Versicherungen Versicherungsschutz auch für Pflichtverletzungen des auf Unternehmensebene gesetzten Rechts (zum Beispiel Satzungen, Richtlinien, Gesellschaftsverträge, Handlungsanweisungen etc.), wenn und soweit die versicherte Person unter objektiver Abwägung aller Umstände annehmen durfte, zum Wohle der Gesellschaft zu handeln.

Einer versicherten Person werden die Handlungen und Unterlassungen anderer Manager nicht zugerechnet (vgl. AVB-GDV 2019, A-7.1).

24.9.2 Laufende Rechtssachen

Der Versicherer ist nicht zur Leistung verpflichtet, wenn der Versicherungsnehmer davon Kenntnis hat, dass ein Versicherungsfall bereits eingetreten ist (vgl. § 2 Abs. 2 S. 2 VVG). Ausgeschlossen sind gemäß A-7 AVB D&O Haftpflichtansprüche, die im Zusammenhang mit Forderungen, Klagen, Verwaltungsakten, Ermittlungsverfahren, Untersuchungen, Urteilen, sonstigen Vollstreckungstiteln oder den diesen zugrunde liegenden Sachverhalten stehen, die bereits vor oder zu Beginn des Vertrages gegen eine versicherte Person oder die Versicherungsnehmerin oder eine Tochtergesellschaft gerichtet waren. Dies bedeutet, dass laufende Rechtssachen nicht vom Versicherungsschutz umfasst werden. Der Ausschluss führt dazu, dass Schadenersatzansprüche aus ehemaligen Streitigkeiten trotz des Anspruchserhebungsprinzips nicht unter die Deckung durch den aktuellen Versicherer fallen (vgl. Ihlas 2017, Rn. 731).

24.9.3 Innenverhältnis

Ansprüche der Versicherungsnehmerin gegenüber versicherten Personen sind ein häufig diskutiertes Thema im Bereich der D&O-Versicherung (vgl. Ihlas 2017, Rn. 634 ff.). Anders als Außenverhältnisansprüche, also Ansprüche Dritter, werden Innenverhältnisansprüche oftmals eingeschränkt und ausgeschlossen (vgl. Ihlas 2017, Rn. 634). In der D&O-Versicherung werden Innenverhältnisansprüche wegen Vermögensschäden aber im Gegensatz zu anderen Haftpflichtpartien trotzdem versichert. So schließt der D&O-Versicherungsschutz weltweit das modifizierte Innenverhältnis ein (vgl. Ihlas 2017, Rn. 635 ff.). In Kontinentaleuropa umfasst der Versicherungsschutz auch oft das erweiterte Innenverhältnis (vgl. Ihlas 2017, Rn. 636).

Das modifizierte Innenverhältnis war schon Bestandteil der ersten Fassung der Musterbedingungen des GDV, den AVB-AVG 1997. Demnach besteht kein Versicherungsschutz, wenn die Innenverhältnisansprüche durch Weisung, Veranlassung oder Beteiligung einer versicherten Person erhoben werden (vgl. Finkel und Seitz 2016, S. 325). Seit den AVB-AVG 2013 fehlt die damalige Begrenzung des Versicherungsschutzes bei Ansprüchen im Innenverhältnis. In den USA besteht der Ausschluss von Innenverhältniansprüchen bis heute (vgl. Ihlas 2017, Rn. 693). Werden hingegen auch Ansprüche, die unter Initiierung einer versicherten Person erhoben werden, versichert, so spricht man vom erweiterten Innenverhältnis (vgl. Ihlas 2017, Rn. 636).

Verstößt beispielsweise ein Vorstand einer Aktiengesellschaft gegen § 93 AktG und die damit verbundenen Pflichten, so kann dies zu Schadenersatzansprüchen der Gesellschaft gegenüber dem Vorstand führen (vgl. § 93 Abs. 2 AktG).

Die Konstellation innerhalb der D&O-Versicherung birgt eine bedeutende Gefahr des Missbrauchs. Die Versicherungsnehmerin hat die Versicherung für den Unternehmensleiter auf fremde Rechnung abgeschlossen. Die Gesellschaft zahlt die Prämie und könnte somit dazu geneigt sein, zusammen mit dem versicherten Unternehmensleiter den

Versicherer in Anspruch zu nehmen (vgl. Ihlas 2017, Rn. 646). Dies bedeutet, dass die Gesellschaft mit dem Unternehmensleiter Absprachen oder Verabredungen trifft, wodurch eine unberechtigte Zahlung durch den Versicherer erfolgt. Diese Manipulation wird auch als „freundliche“, das heißt abgesprochene Inanspruchnahme bezeichnet (vgl. Finkel und Seitz 2016, S. 325). Zur Reduzierung dieses hohen Manipulationsrisikos reagierten einige Versicherer mit einer Gerichtsklausel sowie einer Kündigungs klausel.

Die Gerichtsklausel besagt, dass die Schadenersatzansprüche gerichtlich geltend gemacht werden müssen, damit eine Deckung durch den Versicherer folgen kann. Eine solche Klausel führt dazu, dass die Fälle veröffentlicht werden, was bei einer fiktiven Pflichtverletzung weder im Interesse der Gesellschaft noch des Unternehmensleiters ist (vgl. Finkel und Seitz 2016, S. 325 f.).

Auch die Kündigungs klausel stellt aus Sicht des Versicherers eine Möglichkeit zur Vermeidung einer freundlichen Inanspruchnahme dar. Gemäß der Kündigungs klausel müssen bei Innenhaftungsansprüchen gegenüber dem Unternehmensleiter sowohl die Vorstandsstellung als auch das Dienstverhältnis beendet werden, sofern Leistungen durch den Versicherer verlangt werden (vgl. Ihlas 2003, S. 10). Verschärft wird die Kündigungs klausel durch manche Versicherer, die zusätzlich vorschreiben, dass der Unternehmensleiter nach Kündigung eine Sperr e von fünf Jahren, bezogen auf sämtliche Tätigkeiten der versicherungsnehmenden Gesellschaft sowie Gesellschaften, an denen diese mehrheitlich beteiligt ist, bekommt (vgl. Plück und Lattwein 2004, S. 196). Die Versicherer gehen davon aus, dass bei Vorliegen einer solchen Klausel kein Unternehmensleiter freiwillig seinen Posten aufgibt und sich stattdessen eher gegen die Haftungsansprüche seines Arbeitgebers verteidigt (vgl. Schmitt 2007, S. 172).

In den USA sind Innenansprüche, also Ansprüche der Gesellschaft gegen ihre Organmitglieder, weitgehend vom D&O-Versicherungsschutz ausgenommen. Dies gilt in deutschen Policien ebenfalls für Ansprüche in den USA oder nach dortigem Recht. Der Ausschluss für „insured versus insured“-Ansprüche schließt nicht nur Ansprüche des Versicherungsnehmers oder der mitversicherten Tochtergesellschaften gegen die versicherten Personen vom Versicherungsschutz aus, sondern auch Ansprüche der versicherten Personen untereinander. Der Ausschluss enthält typischerweise einige Wiedereinschlüsse für abgeleitete Ansprüche aus versicherten Ansprüchen, Ansprüche einer versicherten Person aus deren Anstellungsverhältnis, Ansprüche ehemaliger versicherten Personen nach Ablauf einer bestimmten Zeit nach Ausscheiden aus der Gesellschaft sowie Ansprüche von Insolvenzverwaltern, Liquidatoren und dergleichen (vgl. Ihlas 2017, Rn. 657 f.).

24.9.4 Geldstrafen und Bußgelder

Ansprüche wegen Vertragsstrafen, Kautio nen, Bußgeldern und Entschädigungen mit Strafcharakter (punitive und exemplary damages), die gegen die Versicherungsnehmerin oder eine Tochtergesellschaft verhängt oder von ihnen übernommen werden, sind vom Versicherungsschutz ausgeschlossen (vgl. AVB-GDV 2019, Ziffer 7.10).

Der Versicherungsschutz lässt sich für Geldstrafen und Bußgelder erweitern. Mitversichert werden können zu einem die gegen eine versicherte Person auf Basis des Foreign Corrupt Practices Act der USA (Sektion 2(g) (2)(B) des Foreign Corrupt Practices Act, 15 U.S.C. § 78dd- 2(g)(2)(B)) verhängten Strafen. Zum anderen können auch Regressansprüche gegen versicherte Personen wegen Geldstrafen und Bußgeldern mitversichert werden. In diesem Fall ist die Geldstrafe oder das Bußgeld nicht versichert. Wird der Manager aber wegen einer solchen Strafe, die zum Beispiel das Unternehmen zahlen musste, in Regress genommen, besteht Versicherungsschutz. Deckungserweiterungen für Geldstrafen oder Bußgelder wegen fahrlässiger Taten sind am Markt nicht üblich, auch wenn hierfür aus Sicht der versicherten Person durchaus Bedarf besteht.

Im Rahmen anderer Versicherungen (beispielsweise Cyber-Versicherungen) bieten einige Versicherer Versicherungsschutz für Bußgelder an, meist mit dem Zusatz, „soweit rechtlich zulässig“. Es empfiehlt sich insbesondere mit Blick auf die Strafen nach der EU-Datenschutzgrundverordnung, diesen Versicherungsschutz einzukaufen, wenn er angeboten wird. Vom Versicherer sollte vor Vertragsabschluss und nicht erst im Schadenfall eine Erklärung eingeholt werden, wie er die derzeitige Rechtslage in Deutschland zur Frage der Versicherbarkeit von Strafen und Bußen bewertet.

24.10 Fazit

Ein Unternehmensleiter hat als Geschäftsführer, Vorstand oder Mitglied eines Kontroll- oder Beratungsgangs viele Regelungen zu beachten. Die Gesetze wurden in den letzten Jahren immer weiter verschärft. Ein Verstoß gegen gesetzliche Regelungen kann zu einer unbeschränkten persönlichen Haftung des Unternehmensleiters führen, wobei schnell sehr hohe Haftungssummen erreicht werden können.

Die D&O-Versicherung bietet Unternehmensleitern eine gute Absicherung für den Fall, dass gegen sie persönlich ein Haftpflichtanspruch geltend gemacht wird. Unternehmen sollten eine D&O-Versicherung zur Absicherung dieses Risikos abschließen. Zum einen sichern sie ihr Management ab. Zum anderen profitieren sie selbst von der D&O-Versicherung, wenn der D&O-Versicherer ihnen einen begründeten Anspruch gegen die Manager ausgleicht oder ihnen die Kosten einer Freistellung des Managers von Ansprüchen Dritter ersetzt.

Literatur

- Allianz. (2019). Allianz Studie: Fünf Risiken, auf die sich Vorstände im Jahr 2020 einstellen müssen, Pressemitteilung vom 04.12.2019. <https://www.agcs.allianz.com/news-and-insights/news/directors-and-officers-insurance-insights-2020-press-de.html>. Zugegriffen am 22.12.2019.
- AVB-GDV. (2019). Allgemeine Versicherungsbedingungen für die Vermögensschaden-Haftpflichtversicherung von Aufsichtsräten, Vorständen und Geschäftsführern (AVB D&O), Musterbedingungen des GDV, Stand: Mai 2019.

- Dreher, M. (2005). Die Rechtsnatur der D&O-Versicherung. *Der Betrieb*, 58(31), 1669–1675.
- Finanzministerium Niedersachsen. (2002). Lohn- und einkommensteuerliche Behandlung der Beiträge zu Directors & Officers-Versicherungen, Erlass vom 24.01.2002, S 2332 – 161 – 35/S 2245 – 21 – 31 2 (DStZ 2002, 577).
- Finkel, B., & Seitz, B. (2016). *D&O-Versicherung, Kommentar zu den AVB-AVG*. München: C.H. Beck.
- Graf von Westphalen. (2016). Vertragsrecht und AGB Klauselwerke, 13. Kapitel: D&O Versicherung, b) Einzelheiten zur D&O Versicherung, 2016.
- Halm, W., Engelbrecht, A., & Krahe, F. (2015). *Handbuch des Fachanwalts Versicherungsrecht* (5. Aufl.). München: Huchterland.
- Held, F. M. (2006). D&O-Versicherung, 33. Kapitel. In W. Halm, A. Engelbrecht & F. Krahe (Hrsg.), *Handbuch des Fachanwalts, Versicherungsrecht* (2. Aufl.). Neuwied: Luchterhand.
- Ihlas, H. (2003). D&O-Versicherung für das Innenverhältnis dargestellt an Ziffer 1.3 der AVB-AVG des unverbindlichen GDV-Modells. *Haftpflicht international, Recht und Versicherung*, 1–33. <http://www.dr-iHLAS.com/media/referenzen/H/36Phi2003.pdf>.
- Ihlas, H. (2009). *D&O – Directors & Officers Liability*, Duncker & Humblot (2. Aufl.). Berlin: Duncker & Humblot.
- Ihlas, H. (2017). Directors & Officers Versicherung. In Langheid & Wandt (Hrsg.), *Münchener Kommentar zum VVG* (2. Aufl., Bd. 3, S. 2017). München: C.H. Beck.
- Plück, R., & Lattwein, A. (2004). *Haftungsrisiken für Manager: Deckungskonzepte und Praxisbeispiele für Geschäftsführer und Vorstände* (2. Aufl.). Wiesbaden: Gabler.
- Prölss, J., & Martin, A. (2015). *Kommentar zum Versicherungsvertragsgesetz* (Bd. 14, 29., überarb. Aufl.). München: C.H. Beck.
- Säcker, F. J. (2005). Streitfragen zur D&O-Versicherung. *Versicherungsrecht*, 56(1), 10–14.
- Scheifele, B. H. (1993). Die Vermögensschaden-Haftpflichtversicherung für Manager in den Vereinigten Staaten von Amerika, *VVW*.
- Schilling, J. (2007). Wer handelt, der haftet, in: Compliance Report. https://asspromanagerline.de/de/publikationen/comprep_03-2007.pdf. Zugegriffen am 22.12.2019.
- Schmitt, M. S. (2007). *Organhaftung und D&O-Versicherung – Zu haftungs- und deckungsrechtlichen Problemen der Managementhaftung*. München: Utz.
- Schüppen, M., & Schaub, B. (2010). *Münchener Anwaltshandbuch, Aktienrecht, § 24: Haftung von Vorstands- und Aufsichtsratsmitgliedern* (2. Aufl.). München: C.H. Beck.
- Zimmermann, M. (2016). Mögliche Schadensfälle der D&O-Versicherung. <http://www.ich-informiere.de/Managerhaftpflicht/8.html>. Zugegriffen am 22.12.2019.

Marcel Wilms ist seit 2020 Leiter Produktmanagement Haftpflicht Komposit Industrie bei der Gothaer Allgemeine Versicherung AG, zuvor in verschiedenen Positionen bei Versicherungsunternehmen und -maklern, zuletzt Leiter Haftpflicht/Unfall/Kraftfahrt/Rechtsschutz/D&O bei der Deutsche Telekom Assekuranz-Vermittlungsgesellschaft mbH.

Christopher Schatz studiert im Master Risk & Insurance am Institut für Versicherungswesen der Technischen Hochschule in Köln. Neben seinem Studium arbeitet er als Werkstudent beim InsurLab Germany, der größten Brancheninitiative zur Vernetzung von Versicherungsunternehmen und InsurTechs. Seinen Bachelor hat er an der Dualen Hochschule Baden-Württemberg in Mannheim im Fach Betriebswirtschaftslehre mit der Vertiefung Versicherung absolviert. Während dieser Zeit war er als Dualer Student bei der Allianz Beratungs- und Vertriebs AG in Köln beschäftigt.



Risikomanagement in der Supply-Chain

25

Christian Müller und Jan Tschöpe

Zusammenfassung

Der vorliegende Beitrag beschäftigt sich mit der Konzeption des Risikomanagements in der Supply-Chain. Es wird der Frage nachgegangen, welche Ansätze einem erfolgreichen Managen von Supply-Chain Risiken dienen. Ziel ist es zu klären, inwiefern das Risikomanagement der internen Prozesse auf die ganzheitliche Betrachtung des Supply-Chain-Netzwerks übertragbar ist. Zunächst werden die Herausforderungen des Forschungsfeldes herausgearbeitet und verschiedene konzeptionelle Ansätze dargestellt. Anschließend wird das Kernelement, der systematische unternehmensübergreifende Managementprozess zur Identifizierung, Bewertung und Steuerung von Supply-Chain Risiken behandelt. Es werden Methoden für die einzelnen Prozess-Phasen und deren Anwendung im Kontext von Lieferketten beschrieben. Dabei werden ursachenbezogene und wirkungsbezogene Steuerungsmaßnahmen diskutiert. Abschließend wird die Cloudlösung der Continental AG zur Echtzeit-Analyse der Lieferkette vorgestellt, mit der IT-gestütztes Supply-Chain-Risikomanagement illustriert werden kann.

C. Müller (✉)

Conti Versicherungsdienst GmbH, Hannover, Deutschland
E-Mail: christian.2.mueller@conti.de

J. Tschöpe

TH Köln, Institut für Versicherungswesen, Köln, Deutschland
E-Mail: jan-tschoepe@web.de

25.1 Problemstellung und Bedeutung des Supply-Chain-Risikomanagements

Durch die zunehmende Fragmentierung und Vernetzung von Lieferketten steigen die Komplexität von Lieferprozessen und die Abhängigkeit der Unternehmen von Zulieferern. Unterbrechungsrisiken sind für Unternehmen mit stark fragmentierten Lieferketten größer denn je. Seit Jahren entwickelt sich im Zuge der Globalisierung, der Verkürzung der Produktionszyklen sowie der Umsetzung von just-in-time- bzw. just-in-sequence-Konzepten ein Trend zur Verlagerung der Lieferkette auf externe, international operierende Zulieferer, Abnehmer oder sonstigen Dienstleister, sodass die Fertigungstiefe kontinuierlich reduziert wird (vgl. Bayer und Bioly 2014, S. 1; vgl. Zimmer 2017). Mit der Auslagerung von Prozessen oder Verarbeitungsschritten wird grundsätzlich das Ziel verfolgt, bei gegebener Qualität die Kosten zu minimieren bzw. bei gleichbleibenden Kosten die Qualität zu steigern. Dies mündet in der Notwendigkeit, ein Supply-Chain-Netzwerk mit einem komplexen und fragmentierten Ausmaß aufzusetzen. Einerseits wird damit zwar entscheidend die Wettbewerbsfähigkeit des einzelnen Unternehmens erhöht bzw. sichergestellt, andererseits besteht eine signifikante Abhängigkeit von der Leistungsfähigkeit eines solchen Netzwerkes. Aus diesem Grunde bedarf der Umgang mit strategischen und operativen Risiken in solchen Wertschöpfungsketten besonderer Aufmerksamkeit (vgl. Börner und Armon 2015). Die Entwicklung der Wertschöpfungstiefe lässt sich am Beispiel der Automobilindustrie veranschaulichen: Im Rahmen einer Studie des Lehrstuhls für ABWL und Logistik der Universität Marburg wurde die Entwicklung der Hersteller-Zulieferer-Beziehung in der Automobilbranche untersucht. Daraus geht hervor, dass die Fertigungstiefe bei den aufgeführten Automobilherstellern auf nunmehr 30,2 Prozent gesunken ist. In den 1980er- und 1990er-Jahren hingegen lag das Verhältnis der eigenen Produktionsleistung zu der Gesamtleistung des Unternehmens noch zwischen 35 Prozent und 40 Prozent. Zur Untersuchung hinzugezogene Experten gingen im Jahr 2006 von einer mittelfristigen Veränderung der Fertigungstiefe in einem Bereich von 25 Prozent und 30 Prozent aus. Bei einer Fortführung der Studie im Jahr 2015 vermuteten 47 Prozent der Experten, dass die Wertschöpfungstiefe der aufgeführten Unternehmen weiterhin sinken wird (vgl. Göpfert et al. 2016, S. 179 ff.; vgl. Bayer und Bioly 2014, S. 1 f.). Sollte die Verbreitung von Elektrofahrzeugen oder alternativen Antriebstechniken zunehmen bzw. diese die Verbrennungsmotoren in naher Zukunft vom Markt verdrängen, so ist sich eine Vielzahl von Experten einig, dass mit einer deutlichen Reduzierung der Fertigungstiefe zu rechnen ist. Dies ist durch die im Vergleich zu einem Elektrofahrzeug relativ ausgeprägte Komplexität und die höhere Anzahl an Bauteilen eines Verbrennungsmotors begründet (vgl. Göpfert et al. 2016, S. 182 f.).

Darüber hinaus hat die gestiegene Nachfrage nach immer leistungsfähigeren und intelligenteren Produkten und Dienstleistungen dazu geführt, dass die Komplexität in der Leistungserstellung im gleichen Maße steigt (vgl. Harland et al. 2003, S. 51 f.). Der Trend zur Fokussierung auf Kernkompetenzen mündet in der Notwendigkeit, die Produktion und

Produktentwicklung unternehmensübergreifend zu gestalten (vgl. Speckmann und Davis 2004, S. 414 f.). Der dadurch bedingte Anstieg an beteiligten Parteien und Schnittstellen (also potenzielle Ausfallgründe) erhöht gleichzeitig das Risikopotenzial innerhalb der Wertschöpfungskette. Zusätzlich haben sich die Produktlebenszyklen in einigen Branchen drastisch verkürzt, sodass sich die Vorhersehbarkeit der Nachfrage immer schwieriger ermitteln lässt (vgl. Christopher und Lee 2004, S. 388; vgl. Ziegenbein 2007, S. 14).

Da die Verknüpfung unternehmensinterner sowie- übergreifender Prozesse in den Bereichen Material-, Dienstleistungs-, Finanz- oder Informationsströmen von einer erheblichen Komplexität geprägt ist, können diese nur mit der Unterstützung einer umfangreichen IT-Infrastruktur ablaufen. Kommt es zu einem Ausfall der IT-Systeme (unabhängig davon, ob dieser innerhalb des Unternehmens oder entlang der Supply-Chain auftritt) können massive negative Auswirkungen die Folge sein (vgl. Pfohl et al. 2008a, S. 25).

Zudem gilt: Je verflochtener und ausgeprägter die Verknüpfung zwischen unternehmensinternen- und -externen Prozessen ist, desto komplexer wird die Kontrolle und Steuerung darüber (vgl. Speckmann und Davis 2004, S. 416). Ferner werden ein kontinuierlicher Informationsabgleich zwischen den Unternehmen und innerhalb der Supply-Chain wirkende Risikosteuerungsmaßnahmen schwieriger umsetzbar, sodass zahlreiche Risiken und Gefahren schlichtweg unentdeckt bleiben (vgl. Kersten et al. 2006b, S. 243).

Die aufgeführten Trends bedingen zwar große Chancen, erhöhen allerdings bestehende Risiken und lassen neue entstehen, wodurch die Zielerreichung des Wertschöpfungsnetzwerkes und der einzelnen Unternehmen entscheidend beeinflusst werden könnte (vgl. Pfohl 2007, S. 1137). Doch nicht nur die Entwicklungen innerhalb der Supply-Chain, sondern auch die unvorhersehbaren Umweltbedingungen tragen zu einer höheren Fragilität und Empfindlichkeit bei (vgl. Svensson G. 2000, S. 733). Unerwartete signifikante Absatzzückgänge, Insolvenzen von Lieferanten, Streiks, Naturkatastrophen, Cyber-Angriffe, Terroranschläge, Epidemien und andere Ereignisse sind Beispiele für Bedrohungen, die von außen auf das Unternehmen einwirken können. Der Eintritt der genannten Schadenszenarien kann jedoch nicht nur bei dem betreffenden Unternehmen zu Unterbrechungen führen, sondern verursacht eventuell auch bei vor- und/oder nachgelagerten Unternehmen innerhalb der Supply-Chain Unterbrechungsschäden (vgl. Kajüter 2015, S. 13).

Eine explorative Studie liefert den empirischen Beleg dafür, dass das Risikomanagement in den meisten Organisationen als eine unternehmensspezifische Aufgabe interpretiert und umgesetzt wird (vgl. Kajüter 2015, S. 14). Der vorliegende Beitrag zielt darauf ab, ein grundlegendes Verständnis über das unternehmensübergreifende Management von Risiken zu vermitteln. Dazu folgt zunächst eine Darstellung verschiedener konzeptioneller Ansätze des Risikomanagements in der Supply-Chain und im Anschluss die der einzelnen Schritte des Risikomanagementprozesses. Dabei handelt es sich jeweils um eine Kurzbeschreibung der Risikoanalyse und der möglichen Steuerungsmaßnahmen, die als Lösungskonzepte zur Bewältigung der Risiken innerhalb der Supply-Chain im Unternehmen integriert werden können.

25.2 Konzeptionelle Ansätze des Risikomanagements in der Supply-Chain

Die Basis für die Konzeption und Etablierung eines unternehmensübergreifenden Risikomanagements ist eine einheitlich verstandene Strategie risikobezogener, gemeinsamer Zielsetzungen über alle Akteure der Wertschöpfungskette hinweg (vgl. Horvath und Gleich 2000, S. 112). Interessanterweise ist das ein, wenn nicht sogar das Kernproblem, welches über Erfolg oder Scheitern eines Konzeptes entscheidet. Grundsätzlich müssten alle involvierten Parteien dasselbe Interesse verfolgen: einen Schaden und somit eine Liefer-/Produktionsunterbrechung zu vermeiden oder die Auswirkungen eines bereits eingetretenen Risikos zu vermindern.

Grundsätzlich lässt sich der idealtypische Aufbau des Supply-Chain Risk Managements (SCRM) in drei unterschiedliche Ausprägungen differenzieren, wobei die jeweiligen Grenzen in der Praxis fließend sein können (vgl. Kajüter 2015, S. 22). Die Konzeption hängt dabei überwiegend von den Einflussfaktoren Struktur der Lieferkette, Risikopräferenz, Produktionstechnologien, Abhängigkeit und Erfahrung der Zulieferer, der Intensität der Vernetzung der einzelnen Unternehmen, der Umweltkomplexität sowie der Branche ab (vgl. Giunipero und Eltantawy 2004, S. 699). Daher muss sich für jedes Supply-Chain-Netzwerk ein für sich passendes Risikomanagement mit geeigneten Instrumenten entwickeln, das sich an den individuellen Verhältnisse des jeweiligen Unternehmensnetzwerks orientieren muss (vgl. Cuccheilla und Gastaldi 2006, S. 700 f.).

Ausprägungsformen des Supply-Chain-Risikomanagements

Risikomanagement mit Supply-Chain Orientierung stellt einen Teil des allgemeinen Risikomanagements eines einzelnen Unternehmens dar. Die von der Supply-Chain ausgehenden Risiken werden zwar hinsichtlich einer systematischen Identifizierung, Bewertung und Steuerung analysiert, allerdings liegt der Fokus auf Bereichen, wie zum Beispiel der Beschaffung, die einen engen Bezug zu den Material-, Waren- und Informationsflüssen haben. Die Sicherstellung der Versorgung, Qualität sowie die Einhaltung der Kosten stehen im Mittelpunkt. Das Risikomanagement des einzelnen Unternehmens bildet den Schwerpunkt dieses Ansatzes, sodass zugleich die Kooperationsintensität zwischen den Supply-Chain-Partnern im Risikomanagement sehr gering bis gar nicht ausgeprägt ist. Aufgrund der mangelnden Bereitschaft zum Austausch von Informationen sind die Informationsasymmetrien in Bezug auf Risiken als hoch anzusehen. Eine gemeinsame Umsetzung von Zielen und Planungsprozessen hinsichtlich eines kooperativen Risikomanagements ist nicht existent, das notwendige Vertrauen zwischen den Akteuren ist gering (vgl. Kajüter 2015, S. 21 f.; vgl. Pfohl et al. 2008a, S. 28 f.).

Risikoanalyse in der Supply-Chain (Dyadisches Supply-Chain Risikomanagement) zeichnet sich aus durch ein Risikomanagement zwischen einzelnen vor- und nachgelagerten Unternehmen unterschiedlicher Wertschöpfungsstufen mit einer mittleren Kooperati-

onsintensität. Die risikobezogene Zusammenarbeit erfolgt unregelmäßig und informell, sodass die Informationsasymmetrien gemildert werden. Das Verhältnis zwischen den Partnern wird intensiviert und entwickelt sich von einer rein transaktionsorientierten zu einer partnerschaftlichen Beziehung, die von einem höheren Vertrauen gekennzeichnet ist. Ein gemeinsamer Zielsetzungs- und Planungsprozess für die Supply-Chain besteht jedoch nicht oder höchstens zwischen einzelnen Partnerunternehmen (vgl. Kajüter 2015, S. 22; vgl. Norrman und Jansson 2004, S. 450 f.; vgl. Pfohl et al. 2008a, S. 28 f.). Insgesamt findet dieser Ansatz in der Realität selten bis nie Anwendung. Bisweilen wird höchstens von einem zentralen Unternehmen innerhalb der Supply-Chain vorgeschrieben, welche Pflichten die verbundenen Partner bezüglich des Risikomanagements einzuhalten haben (vgl. Pfohl et al. 2008a, S. 29).

Supply-Chain-Risikomanagement (Netzwerkweites Supply-Chain-Risikomanagement) betrachtet hingegen die gesamte Wertschöpfungskette, in der sämtliche beteiligte Partner miteinander in Kooperation stehen. Ein regelmäßiger Austausch von Risikoinformationen innerhalb des Netzwerks führt zu einer geringen Ausprägung der risikobezogenen Informationsasymmetrien. Da die Festlegung und Umsetzung von Zielen sowie Planungsprozesse gemeinsam stattfinden, sind die Beziehungen von einem partnerschaftlichen Verhältnis und zugleich hohem Vertrauenspotenzial zwischen den Akteuren gezeichnet (vgl. Pfohl et al. 2008a, S. 29). Um die Koordination der Aktivitäten zu steuern, kann innerhalb des Supply-Chain-Netzwerks ein Gremium, bestehend aus Vertretern aller Partner der Lieferkette, zusammengestellt werden (vgl. Kersten et al. 2006a, S. 14). Ein solches Gremium birgt zwar hohes Konfliktpotenzial in sich, gewährleistet jedoch zum einen einen regelmäßigen Austausch von risikobezogenen Informationen der Supply-Chain-Mitglieder, zum anderen ist es auch für die Entscheidungen über die Steuerung von Risiken innerhalb der Wertschöpfungskette verantwortlich (vgl. Pfohl et al. 2007, S. 214).

Welcher dieser aufgeführten Ansätze sich zur Umsetzung des Risikomanagements eignet, hängt im Wesentlichen davon ab, auf welche Art und Weise die Geschäftsbeziehung zwischen den einzelnen Partnern der Supply-Chain aufgebaut ist und in welcher Intensität die Kooperation der Unternehmen stattfindet. Da zusätzlich die Phase der Netzwerkbildung für die Entscheidung relevant ist, mit welchen anderen Akteuren sie wie intensiv kooperieren, können die drei Ausprägungen des Risikomanagements auch parallel Anwendung finden. Mit Zunahme der Kooperationsintensität und Interaktion in der gemeinsamen Analyse und Steuerung der Risiken, kann eine schrittweise Entwicklung von einem unternehmenseigenen Risikomanagement mit Supply-Chain-Orientierung über eine unternehmensübergreifende Risikoanalyse bis hin zu einem integrierten und netzwerkweiten Supply-Chain-Risikomanagement erfolgen (vgl. Kajüter 2015, S. 22 f.).

Das Kernelement eines Risikomanagements in Supply-Chains ist das Konzept des gemeinsamen Risikomanagementprozesses. Im Folgenden werden die einzelnen Phasen des Risikomanagementprozesses vertiefend beschrieben, indem insbesondere der grundlegende Prozessablauf und die dazugehörenden Methoden dargestellt werden.

25.3 Prozess des Risikomanagements in Supply-Chains

25.3.1 Bildung risikobezogener Zielsetzungen als Ausgangspunkt des Risikomanagements

Um ein optimales Managen von Risiken zu gewährleisten, stellen für alle Unternehmen der Lieferkette die risikobezogenen Überlegungen im Zusammenhang mit den verfolgten Zielen eine grundlegende Voraussetzung dar. Sie geben unter anderem die Risikodefinition vor, legen Sicherheitsziele hinsichtlich bestimmter Risiken fest und bestimmen risikopolitische Maßnahmen, die zur Absicherung dienen. Zu berücksichtigen ist hierbei auch, dass die Partner innerhalb der Supply-Chain zum einen verschiedene oder gar konkurrierende Risikopräferenzen aufweisen und zum anderen einen unterschiedlichen Umgang mit Risiken pflegen. Die Zielabstimmung wird dabei unmittelbar beeinflusst (vgl. Götze und Mikus 2015, S. 31; vgl. Kajüter 2003, S. 111). Die Herausforderung hierbei besteht darin, in welcher Form sich das Risiko bzw. die Unsicherheit in den risikobezogenen Zielen des Supply-Chain Managements (SCM) aufzeichnen lässt und wie dies in Zielbildungsprozessen erfolgen kann. Zudem bilden die Überlegungen des Risikomanagements auch eine Basis für das SCM, da das Risiko in vielen Zielbildungsprozessen eine maßgebliche Rolle spielt und eine Zielharmonisierung entscheidend den Erfolg bestimmt (vgl. Götze und Mikus 2015, S. 31).

Insgesamt bestehen mehrere alternative oder einander ergänzende mögliche Strategien das Risiko in das Zielsystem zu integrieren, die sich ebenso auf das SCM übertragen lassen. Als übergeordnetes Ziel, welches in Verbindung mit dem Risikomanagement als generelles Sicherheitsstreben ausgewiesen wird, gilt vorerst die „Sicherung der Unternehmensexistenz“. Analog zur Unternehmensführung einzelner Partner stehen auch im Rahmen des SCM verschiedene risikobezogene Grundstrategien zur Auswahl. Diese geben Auskunft über die Risikopräferenz der Entscheidungsträger und legen die Grenzen des Eingehens von Risiken fest (vgl. Götze und Mikus 2015, S. 32 f.).

Grundsätzlich wird zwischen der statisch-adaptiven und der dynamisch-aggressiven Strategie unterschieden. Die statisch-adaptive Strategie zielt auf die umfangreiche Bereitstellung von Ressourcen ab und ist daher von geringem Risiko und hohen Kosten gekennzeichnet. Das Gegenstück, die dynamisch-aggressive Strategie, zeichnet sich hingegen durch hohe Gewinnchancen bei gleichzeitig größeren Risiken aus. Eine Risikobegrenzung innerhalb der Wertschöpfungskette erfolgt bereits bei der Erfüllung der „allgemeinen“ Supply-Chain-Ziele (vgl. Götze und Mikus 2015, S. 32 f.).

Im Rahmen des SCM lassen sich Formal- und Sachziele kategorisieren. Formalziele können übergeordnete Ziele wie Gewinnmaximierung und Wachstum sein. Sachziele richten sich konkret auf die Durchführung der Supply-Chain-Aktivitäten und bestimmen maßgeblich die Erfüllung der Formalziele. Die Sachziele lassen sich untergliedern in Leistungsziele (zum Beispiel Sicherstellung der Wettbewerbsfähigkeit oder Gewährleistung der Versorgungssicherheit), Finanzziele (zum Beispiel Fokussierung von Kostensenkungen entlang der Fertigungsstufen und niedriger Kapitalbindung) und Sozialziele (Berück-

sichtigung der Sozial- und Ökologieumwelt). Einige dieser Ziele tragen bereits zur Reduzierung von Risiken bei, sodass sie teilweise auch als eigenständige Sicherheitsziele deklariert werden können. Zuletzt ist noch die Unsicherheit als Zieldimension aufzuführen. Wird Unsicherheit in die Entscheidungsfindung integriert, so wird für sämtliche Größen des Zielsystems eine (Un-) Sicherheitspräferenzrelation festgelegt, die sich nach der Risikobereitschaft der Entscheidungsträger richtet (vgl. Götze und Mikus 2015, S. 33).

Basierend auf den beschriebenen Ansatzpunkten ist individuell zu bestimmen, inwie weit eine Thematisierung bzw. Integration derselben in den risikobezogenen Zielbildungsprozess erfolgen soll. Bezogen auf das Risikomanagement in einer Supply-Chain sind die beteiligten Partner stets hinsichtlich ihrer Interessen und Beteiligung zu berücksichtigen. Aufgrund der differenzierten Risikoeinstellungen sollten die risikobezogenen Zielvorstellungen idealerweise nach den vier aufgeführten Zieldimensionen gegliedert werden, um die Abstimmungsprozesse zwischen den Unternehmen zu erleichtern (vgl. Götze und Mikus 2015, S. 33 f.).

25.3.2 Risikoanalyse

25.3.2.1 Systematisierung von Risiken

Da die Kategorisierung von Risiken eine wichtige Grundlage darstellt, um diese gezielt zu identifizieren und analysieren, wird nachfolgend ein Überblick über die Supply-Chain-bezogene Klassifizierung der Risikoarten dargestellt (vgl. Götze und Mikus 2015, S. 35). Aufgrund der verschiedenen Kategorisierungsmöglichkeiten in der Literatur ist es kaum möglich, eine klare Systematisierung vorzunehmen. Es gibt eine Vielzahl von Kriterien, anhand derer sich die Risikoarten differenzieren lassen (vgl. Pfohl et al. 2008a, S. 21 f.).

Eine gebräuchliche Systematisierung von Supply-Chain-relevanten Risiken erfolgt anhand der Differenzierung des Entstehungsortes. Abhängig davon, ob sich die Risikoursache innerhalb oder außerhalb des Unternehmens befindet, ist zwischen innerbetrieblichen (endogenen) und außerbetrieblichen (exogenen) Risiken zu unterscheiden. Diese Abgrenzung gilt es in Bezug auf das SCRM zu erweitern, indem man diejenigen Risikoursachen unterscheidet, die sich innerhalb der Supply-Chain selbst und diejenigen, die sich außerhalb der Supply-Chain befinden. Liegt die Risikoursache in der Wertschöpfungskette selbst, so kann sie weiterhin unternehmensübergreifend und unternehmensintern begründet sein. Insgesamt können also folgende drei Risikoarten auftreten: Supply-Chain-exogene, unternehmensübergreifende Supply-Chain-endogene sowie unternehmensbezogene Supply-Chain-endogene Risiken (vgl. Götze und Mikus 2015, S. 35; vgl. Jüttner et al. 2003, S. 201 f.).

Da Entscheidungen des Supply-Chain-Managements vor allem Produkte, Prozesse, Ressourcen sowie Kooperation als Gegenstand haben, kann man nach Entscheidungsobjekten in produkt-, prozess-, ressourcen- und kooperationsbezogenen Risiken kategorisieren. Hierbei handelt es sich überwiegend um endogene Risiken (vgl. Götze und Mikus 2015, S. 35).

Eine weitere sinnvolle Unterscheidung ergibt sich insbesondere hinsichtlich der Prozesse und Ressourcen. Die prozessbetreffenden Risiken lassen sich nach Prozessarten systematisieren, um daraus verschiedene Risikoarten abzuleiten. Demnach lassen Risiken, die sich auf die Kernprozesse Planung, Beschaffung, Produktion, Lieferung und Entsorgung beziehen, strukturieren (vgl. Mikus 2003, S. 151 ff.).

Ferner stellen logistische Risiken aufgrund ihrer thematischen Relevanz ein geeignetes Kriterium zur Differenzierung der Risikoarten dar. Nach den logistischen Abläufen sind hierbei speziell die Risiken der Lagerung, Verpackung, Transport sowie der Auftragsabwicklung aufzuführen (vgl. Götze und Mikus 2015, S. 36 f.; vgl. Pfohl 2010, S. 66 f.).

Eine weitere Klassifizierung von Risiken lässt sich anhand von Ergebnisabweichungen vornehmen. Hierbei wird eine Unterscheidung zwischen reinen und spekulativen Risiken getroffen. Reine Risiken können vom Zielwert nur in eine Richtung abweichen. Die spekulativen Risiken hingegen können sowohl positive als auch negative Ausprägungen annehmen. Das reine Risiko lässt sich anhand des Beispiels der Ertragssteuersenkung illustrieren. Als Beispiel für speulative Risiken kann der Eintritt in neue Beschaffungsmärkte aufgeführt werden. Diese Maßnahme kann zur Reduzierung von Kosten beitragen, gleichzeitig aber auch eine Gefährdung der kontinuierlichen Versorgung auslösen. Will man die Supply-Chain-bezogenen Risiken im zeitlichen Kontext betrachten, so kann man zwischen Risiken unterscheiden, die permanent und zeitlich begrenzt sind. Ausgehend von der Tragweite der Risiken und der allgemeinen Risikopräferenz der Unternehmen ist auch eine Differenzierung zwischen Bagatellrisiken, kleinen, mittleren, großen und existenzbedrohende Risiken möglich (vgl. Gabath 2010, S. 35).

Abschließend ist die Abhängigkeit von der Entscheidungsebene zu erwähnen, die es erlaubt, strategische, taktische und operative Risiken zu trennen. Während die strategischen Risiken das gesamte Unternehmen betreffen und die Realisierung von langfristigen und globalen Zielen negativ beeinflussen, beziehen sich operative Risiken auf einen mittel- bis kurzfristigen Zeithorizont. Abhängig vom Umfang der Entscheidungen lassen sich Einzelrisiken von Gesamtrisiken unterscheiden. Einzelrisiken spiegeln das bewirkte Risiko einer Entscheidung wider, Gesamtrisiken hingegen beziehen sich auf die Gesamtheit der getroffenen Entscheidungen (vgl. Lasch et al. 2015, S. 80).

Im folgenden Abschnitt werden die in der Phase der Identifikation verwendeten Methoden näher betrachtet. Eine solche Analyse bedingt vor allem Kenntnisse bzw. die Beherrschung von Strukturierungsmethoden, weshalb ebenso ausgewählte Methoden zur Identifikation von Supply-Chain-Risiken dargestellt werden. Zusätzlich wird das generelle Vorgehen der Ursache-Wirkungs-Analyse beschrieben, um die Grundlage für eine präzise Risikobewertung und letztlich für die Auswahl von entsprechenden risikopolitischen Steuerungsmaßnahmen zu legen.

25.3.2.2 Identifikation von Risiken und risikoauslösenden Faktoren

Ausgewählte Methoden zur Identifizierung von Risiken

Der gemeinsamen Risikoidentifikation und -analyse von risikoauslösenden Faktoren, welche die erste Teilphase der Risikoanalyse bilden, wird im Supply-Chain-Risikomanagement

eine besondere Bedeutung zugesprochen. Die zentrale Aufgabe liegt dabei in der vollständigen, rechtzeitigen und wirtschaftlichen Erfassung aller potenziellen Risiken entlang der Lieferkette und deren auslösenden Ursachen, um eine Aussage über ihre Relevanz für die Supply-Chain zu treffen (vgl. Jung und Nowitzky 2006, S. 61 f.). Erfolgt ein unternehmensübergreifendes Supply-Chain-Risikomanagement, so hängt die Wirksamkeit maßgeblich von der gemeinsamen Auffassung der potenziellen Risiken und der strukturierten und kommunizierten verfolgten Risikostrategie aller Kooperationspartner ab, die den Fokus auf eine präventive Krisenabwehr legen sollte. Damit alle beteiligten Unternehmen der Lieferkette die Supply-Chain-bezogenen Risiken identifizieren können, muss folglich eine grundlegende und gültige Systematik zwischen allen Akteuren bestehen (vgl. Pfohl et al. 2008a, S. 36).

Für die systematische Erfassung und Identifizierung risikobezogener Faktoren besteht eine Vielzahl von Suchstrategien und Verfahren. So kann an der Entstehung der Risiken angesetzt und als Ausgangspunkt die Kategorisierung von Risiken verwendet werden. Daraus geht hervor, dass sowohl die Umwelt der Lieferkette als auch die unternehmensübergreifenden Wertschöpfungsbereiche und einzelne Akteure des Netzwerks in die Suche miteinbezogen werden sollten. Als weiteren Ansatzpunkt können die verfolgten Ziele sowie die zu treffenden Entscheidungen dienen. In diesem Zusammenhang gilt es zu untersuchen, von welchen Faktoren eine Gefährdung der zeitraumbezogenen, allgemeinen oder spezifischen verfolgten Supply-Chain-Zielen ausgeht (vgl. Götze und Mikus 2015, S. 41).

Grundsätzlich lassen sich die Methoden zur Identifizierung Supply-Chain-bezogener Risiken in Kollektions- und Suchmethoden gliedern. Kollektionsmethoden werden zur Entdeckung von bestehenden und offenkundigen Risikopotenzialen eingesetzt. Suchmethoden hingegen zielen auf die Identifizierung zukünftiger und bislang unbekannter Risiken ab und leisten dabei einen wichtigen Beitrag für ein proaktives Risikomanagement (vgl. Pfohl et al. 2008a, S. 37).

Unter den Kollektionsmethoden lassen sich die Stärken-Schwächen-Analyse, Risiko-identifikationsmatrix, Risikochecklisten, Interviews und Befragungen von Experten bzw. Mitarbeitern, Dokumentationsanalysen sowie Betriebsinspektionen einordnen. Bei den Suchmethoden lassen sich analytische Methoden von Kreativitätmethoden unterscheiden. Zu den analytischen Methoden zählen unter anderem Fragenkataloge, morphologische Verfahren, qualitative- und quantitative Prognoseverfahren sowie Prozess- und Ausfallkettenanalysen. Unter den kreativen Methoden befinden sich vor allem verschiedene Techniken des Brainstormings und Schätzverfahren, die dazu dienen, zukünftige Trends und technische Entwicklungen zu erkennen. Darauf hinaus lassen sich noch weitere spezielle Methoden aufführen, die eine besondere Supply-Chain-Orientierung aufweisen (vgl. Pfohl et al. 2008a, S. 37).

Ein strukturierter Ansatz, der zur Entdeckung von Risikoquellen beiträgt und dabei auch die Konsequenzen daraus miteinbezieht, stellt die Supply-Chain-Risk-Map dar (vgl. Norrman und Lindroth 2004, S. 21). Hierbei wird prinzipiell die zusammenhängende Vernetzung der einzelnen Supply-Chain-beteiligten Mitglieder grafisch dargestellt. In die Betrachtung einbezogen werden insbesondere der zeitliche Fluss von Materialien, Komponenten und

Produkten entlang der Wertschöpfungskette vom Rohstofflieferanten bis hin zum Endkunden. Ziel dieser Methode ist zum einen, die kritischen Supply-Chain Mitglieder bzw. Prozesse ausfindig zu machen, da sie zum Beispiel eine hohe Sensibilität in der Zeitplanung bzw. wenige bis keine Zeitredundanzen aufweisen. Zum anderen sind dadurch Alternativen der Beschaffungsstrategien zu regeln und Entscheidungen hinsichtlich alternativer Lagerhaltungs- und Transportmöglichkeiten festzulegen (vgl. Pfohl et al. 2008a, S. 38).

Eine weitere Möglichkeit zur Identifizierung von Supply-Chain-Bedrohungspotenzialen stellen Betriebsinspektionen der Netzwerkpartner dar, zum Beispiel im Rahmen kontinuierlicher Risiko-Audits. Bedrohungen auf der Beschaffungsseite lassen sich unter anderem im Rahmen von Lieferantenaudits ermitteln. Im Zusammenhang mit Betriebsbesichtigungen auf Supply-Chain-Ebene kann eine Überprüfung der Prozesssicherheit des Lieferanten erfolgen, um die Existenz von Alternativprozessen für Notfallsituationen sicherzustellen. Auf Basis dieser Informationen kann abschließend eine Bewertung erfolgen, ob eine Bereitschaft der Lieferanten zur Handhabung von unvorhersehbaren Bedrohungen sowie die geplanten Rektionsmaßnahmen zur Bewältigung der Risiken vorhanden sind (vgl. Zsidisin et al. 2005, S. 49 f.).

Ursache-Wirkungs-Analyse

In der zweiten Teilphase der Risikoanalyse geht es darum, die identifizierten Risiken und risikoauslösenden Faktoren einer Ursache-Wirkungs-Analyse zu unterziehen. Diese dient der Vorbereitung für die nachfolgende Bewertung der Risiken sowie der Konzeption und auch Auswahl risikobezogener Steuerungsmaßnahmen (vgl. Götze und Mikus 2015, S. 42).

Sie umfasst die Spezifizierung und Analyse einzelner Risikoquellen, um unter anderem zu ermitteln, bei welcher Ausprägung des entsprechenden Risikos eine negative Auswirkung auf die Zielerreichung eintritt und wie bzw. ob dieses Risiko steuerbar ist. Zudem werden die risikoauslösenden Faktoren entlang der Lieferkette, welche von verschiedenen Supply-Chain-Akteuren ausgehen können, in Form einer Analyse der Ursachen-Wirkungsbeziehungen untersucht, inwieweit Risikoursachen miteinander verknüpft sind. Weiterhin erfolgt eine Prognostizierung, wie direkte und indirekte Effekte der Risiken die Planungsprozesse und darüber die Zielerreichung beeinflussen können. Abschließend werden die Eintrittswahrscheinlichkeiten risikobestimmender Entwicklungen und Vorfälle in subjektiver sowie objektiver Hinsicht ermittelt, um den Grad der Unsicherheit bezüglich des Eintritts und/oder der Effekte der jeweiligen Risiken zu reduzieren (vgl. Götze und Mikus 2015, S. 42).

Die Analyse und Prognose der möglichen Risikofolgen lassen sich in unterschiedlichen Reichweiten umsetzen. Zum einen können isoliert die Wirkung eines risikobezogenen Faktors oder die konsolidierten Auswirkungen mehrerer Risikoquellen betrachtet werden. Zum anderen kann aber ebenso das Abweichen einer Zielerreichung bei der Entscheidung bezüglich einzelner Risiken oder das aus den Wirkungen mehreren bzw. allen aggregierten Entscheidungen entstehende Gesamtrisiko (des eigenen Unternehmens oder der gesamten Supply-Chain) als Gegenstand der Untersuchung dienen (vgl. Götze und Mikus 2015, S. 42 f.; vgl. Mikus 2009, S. 172 ff.).

Zudem lässt sich feststellen, dass auf Grundlage der Identifizierung der Wirkungsorte der Risikofaktoren ebenso die Auswirkungen, welche sowohl das eigene Unternehmen als auch unternehmensübergreifend die gesamte Lieferkette betreffen bzw. für die Erreichung der einzelnen Unternehmensziele relevant sind, zu prognostizieren und zu analysieren sind. Hierbei sollte nicht nur auf unternehmensspezifischen Untersuchungsinstrumentarien zurückgegriffen werden, sondern auch die Analyse der Supply-Chain-bezogenen Wirkungen miteinbezogen werden, um eine Bewertung und Steuerung der Risiken aus Sicht der einzelnen Partner und der gesamten Lieferkette zu gewährleisten (vgl. Götze und Mikuš 2015, S. 43).

25.3.2.3 Risikobewertung

Für die Risikobewertung gibt es eine Vielzahl unterschiedlicher Methoden, wobei aufgrund der vielschichtigen Risiken oftmals mehrere Bewertungsinstrumentarien miteinander zu kombinieren sind (vergleichbar mit dem Prozess der Risikoidentifizierung) (vgl. Etterer 2008, S. 199). Da die gewonnenen Erkenntnisse aus der Phase der Identifizierung von Risiken die Basis für die Risikobewertung darstellen, hat die Qualität sowie die Verfügbarkeit der Daten für dessen Umsetzung eine besondere Bedeutung (vgl. Buchhart und Burger 2001, S. 101). Das übergeordnete Ziel der Risikobewertung ist es, die Supply-Chain-bezogenen Risiken möglichst vollständig und kontinuierlich zu quantifizieren. Die Schwierigkeit dabei besteht darin, das im Unternehmen bestehende implizite Wissen nutzbar zu machen und in die Bewertungsphase zu integrieren. Prinzipiell sind gleiche Risikoarten über alle Unternehmen hinweg mit den identischen Verfahren und Kennzahlen zu bewerten, sodass eine Vergleichbarkeit der Resultate gewährleistet werden kann (vgl. Pfohl et al. 2008b, S. 124).

Die Bewertungsmethoden lassen sich in mehrere Ansätze gliedern: Qualitative Verfahren umfassen die Bewertung von Risiken, bei denen weder die Eintrittswahrscheinlichkeiten noch die daraus ableitbaren Erwartungswerte vorhanden sind (vgl. Fiege 2006, S. 175). Eine exakte Ermittlung des Schadenspotenzials ist hierbei nicht möglich. Als Beispiele lassen sich hierbei Portfolio-Ansätze, Scoring-Modelle, Schätzungen sowie Experteninterviews aufführen. Bei quantitativen Bewertungsansätzen hingegen ist das Ausmaß eines etwaigen Risikoeintrittes konkret zu beziffern. Sie spielen vor allem bei der Verknüpfung des Supply-Chain-bezogenen Risikomanagements mit der Wertorientierung des Unternehmens eine Rolle, da neben den Zielen auch parallel die Risiken in monetären Geldeinheiten ausgedrückt werden können. Beispiele für quantitative Bewertungsverfahren sind Sensitivitätsanalysen, Value-at-Risk-Berechnungen, Kennzahlensysteme sowie Szenario-Analysen (vgl. Buchhart und Burger 2001, S. 102; vgl. Pfohl et al. 2008b, S. 124). Als dritten Bewertungsansatz lassen sich die semi-quantitativen Methoden aufführen. Sie lassen sich mit den qualitativen Methoden kombinieren, sodass belastbare Zahlen mit allgemeinen Einschätzungen verknüpft werden können (vgl. Bayer und Bioly 2014, S. 32). Hierunter verorten sich beispielsweise die Fehlermöglichkeits- und Einflussanalysen sowie die Fehlerbaumanalysen (vgl. Pfohl et al. 2008a, S. 51).

In einer explorativen Studie wurden 160 Industrie-, Handels- und Logistikunternehmen nach der generell bestehenden und zukünftigen Risikosituation in der Supply-Chain sowie der Handhabung Supply-Chain-bezogener Risiken befragt. Dabei konnten unter anderem die unterschiedlichen Präferenzen hinsichtlich der Häufigkeit des Einsatzes und der Eignung von Bewertungsverfahren ermittelt werden. Die Befragten konnten die Eignung der zur Auswahl stehenden Bewertungsmethoden mithilfe einer fünfstufigen Likert-Skala mit den Abstufungen von „eignet sich voll“ bis „eignet sich gar nicht“ bewerten. Aus den Ergebnissen ging hervor, dass zur Bewertung Supply-Chain-bezogener Risiken oft auf qualitative Verfahren wie zum Beispiel Schätzverfahren und Experteninterviews zurückgegriffen wird. Am häufigsten kommt in Industrie- und Handelsunternehmen sowie bei Dienstleistern die Verwendung von Kennzahlensystemen zum Einsatz. Ansätze, wie zum Beispiel Risikosimulationen, Scoring-Modelle oder Sensitivitäts-Analysen, die einen besonderen Aufwand bedürfen, spielen in der praktischen Anwendung bei den befragten Unternehmen nur eine geringe Rolle. Obwohl der Großteil der Befragten die Aussage tätigte, dass sich Schätzverfahren nicht zur Bewertung von Supply-Chain-Risiken eignen, sind diese in der Praxis sehr häufig im Einsatz (zwischen 78 Prozent und 80 Prozent). Die hohe Verbreitung liegt neben dem geringen Aufwand und der möglichen nicht vorhandenen Existenz von detaillierten Daten zur genauen Risikobewertung vor allem in Plausibilitätskontrollen bzw. Misstrauen gegenüber anderen Verfahren, die eine geringere Transparenz aufweisen, begründet (vgl. Pfohl et al. 2008b, S. 124 f.).

Da sich Eintrittswahrscheinlichkeiten und Schadenausmaße für die Auswirkung von Risiken schwer ermitteln lassen, ist es oftmals sinnvoll, diese mithilfe von abgeschwächter und nominaler Beurteilung abzuschätzen. Die getroffenen Beurteilungen der beiden Werte werden dann hinsichtlich des Risikos gemäß der Bedeutung klassifiziert. Es erfolgt eine Kategorisierung in geringe, mittlere oder hohe Risiken oder Bagatellrisiken sowie kleine-, mittlere- und große Risiken oder Existenzrisiken. In Form von Risk-Maps oder Risiko-Portfolios werden die Einschätzungen ihres Zustandekommens visualisiert (vgl. Abb. 25.1). Auf Grundlage dessen und ausgehend vom risikobezogenen „Toleranzbereich“ lässt sich eine Abschätzung über das Ausmaß des jeweiligen Handlungsbedarfs bestimmen. Eine Anwendung auf Supply-Chain-Ebene lässt sich allerdings nicht ohne Weiteres darstellen, da die für die Einschätzung notwendigen Wesentlichkeitsgrenzen in Bezug auf die Risikopräferenzen und -tragfähigkeit der einzelnen Supply-Chain-Mitglieder in der Regel nicht identisch sind bzw. sich häufig erheblich unterscheiden können. Eine mögliche Lösung ist daher, die Risk-Maps zunächst auf Unternehmensebene zu erzeugen und dann ihre Resultate auf Supply-Chain-Ebene mit den Achsen „Unternehmensrisiken“ (mit den Formen A,-, B- und C-Risiken) und „Einfluss auf Supply Chain“ (mit den Werten hoch, mittel, gering) zu projizieren und in einem Supply-Chain-Risikoportfolio zusammenzufassen. Dadurch sollen die identifizierten Risiken der einzelnen Unternehmen für die Lieferkette beurteilt und eine Übersicht über die Supply-Chain-bezogenen Risiken generiert werden (vgl. Götze und Mikus 2015, S. 44 f.).

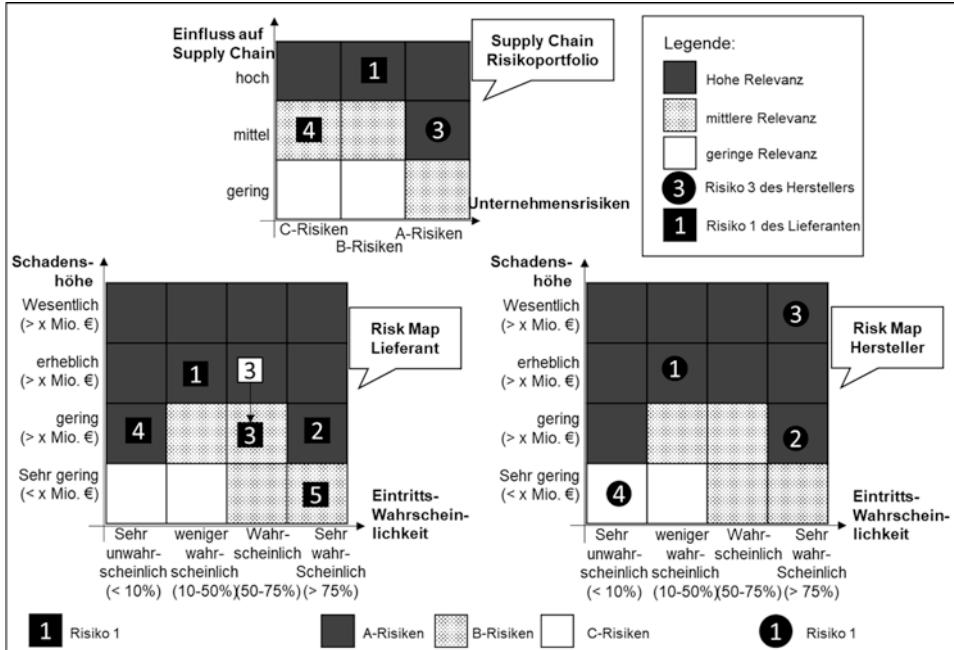


Abb. 25.1 Risk Maps und Supply-Chain-Risikoportfolio. (Quelle: eigene Darstellung in Anlehnung an Kajüter 2003, S. 121)

25.3.3 Steuerung von Supply-Chain-Risiken

Nachdem die Risiken entlang der Supply-Chain bewertet und mithilfe eines Risikoportfolios untersucht wurden, folgt zunächst eine Analyse des Risikoprofils. Hierbei wird zum Beispiel festgestellt, ob die Mehrheit der Risiken unternehmensinternen- oder -externen Prozessen der Lieferkette zuzuordnen ist. Ebenso ist eine vergleichende Analyse der Versorgungsrisiken gegenüber Nachfragerisiken hinsichtlich des Kräfteverhältnisses sinnvoll. Nach den ersten gewonnenen Erkenntnissen lassen sich potenzielle risikopolitische Steuerungsmaßnahmen anhand eines Brainstormings erörtern. Mögliche Handlungsalternativen sind diesbezüglich zu bewerten und zu vergleichen. Insbesondere gilt es zu prüfen, inwieweit sich die vorgeschlagenen Steuerungsmaßnahmen dazu eignen, die Eintrittswahrscheinlichkeit oder das Schadensmaß effektiv zu verringern (vgl. Bayer und Bioly 2014, S. 45; vgl. Jüttner und Ziegenbein 2009, S. 213 f.). Zusätzlich müssen die einzelnen Maßnahmen aus betriebswirtschaftlicher Sicht in Bezug auf die Kosteneffizienz gerechtfertigt sein. Dies erfolgt durch einen Vergleich der Kosten der Steuerungsmaßnahme mit dem potenziellen Schadensausmaß, das beim Eintritt des jeweiligen Risikoereignisses entstehen würde. Insgesamt besteht das Ziel in den meisten Fällen nicht darin, das Risiko vollständig zu eliminieren, sondern auf ein akzeptables Maß zu reduzieren. Die Risikoaversion des Entscheidungsträgers bestimmt die Höhe des angestrebten „Sicherheitsni-

veaus“. Dies ist allerdings als rein subjektiv anzusehen und muss die Einhaltung von geltenden Gesetzen und behördlichen Vorschriften berücksichtigen. Die Entwicklung von Steuerungsansätzen ist folglich vollständig auf die Strategie und Ziele des jeweiligen Unternehmens abzustimmen (vgl. Bayer und Bioly 2014, S. 45; vgl. Kaye 2008, S. 38 f.).

Grundsätzlich lässt sich im Rahmen der Risikosteuerung eine Unterscheidung zwischen ursachenbezogenen und wirkungsbezogenen Maßnahmen vornehmen. Die ursachenbezogenen Maßnahmen zeichnen sich dadurch aus, eine Eliminierung bzw. Reduzierung der Risikoursachen anzustreben, um ein mögliches negatives Abweichen der Zielerreichung zu vermeiden bzw. zu vermindern. Das Ziel der wirkungsbezogenen Maßnahmen ist hingegen, die Folgen eines Eintritts von Risikoursachen zu verringern und damit das Schadenausmaß zu minimieren bzw. einzuschränken. Die Unterscheidung lässt sich zunächst auf reine Risiken anwenden. Bezieht sich diese Differenzierung auf spekulative Risiken, so muss sie „... um das Herbeiführen des Eintretens primär mit Chancen verbundener Risikoursachen sowie um die Erhöhung der positiven Effekte des Eintretens von Risikoursachen“ erweitert werden (vgl. Götze und Mikus 2015, S. 46 f.).

Im Folgenden werden einzelne Steuerungsmaßnahmen vorgestellt, wobei eine klare Abgrenzung zwischen den einzelnen Kategorien nicht immer praktikabel ist. Vor allem die Einordnung einzelner Maßnahmen ist oftmals nicht eindeutig abzugrenzen. Zudem kann es sein, dass Risiken, die während der Identifizierungsphase im Risikomanagement-Prozess nicht entdeckt wurden (unidentifizierte Risiken), implizit bei der Risikosteuerung mitgetragen werden (vgl. Pfohl et al. 2008a, S. 66 f.).

25.3.3.1 Ursachenbezogene Steuerungsmaßnahmen

Wie bereits dargestellt streben ursachenbezogene Steuerungsmaßnahmen eine Verringerung der Eintrittswahrscheinlichkeit von Risikoquellen an. Hierbei wird der Versuch unternommen, mithilfe einer Verbesserung der Informationsbeschaffung einen Abbau der Unsicherheit für die Planungsabteilung zu erreichen (vgl. Mikus 2001, S. 177). Dazu werden über die oftmals risikobezogenen Ursache-Wirkungs-Ketten Informationen in der Lieferkette gesammelt sowie Maßnahmen ergriffen, die bereits bei der Entstehung von Risiken eingreifen sollen. Es wird folglich primär das Ziel verfolgt, eine Veränderung der risikoauslösenden Faktoren zu schaffen, um ein aus dem Risiko resultierendes Ereignis erst gar nicht eintreten zu lassen bzw. dessen Eintrittswahrscheinlichkeit zu vermindern (vgl. Melzer-Ridinger 2001a, S. 45). Generell lassen sich bei der ursachenbezogenen Steuerung die Maßnahmen zur Risikovermeidung von den Maßnahmen zur Risikominderung unterscheiden.

Risikovermeidung

Risikovermeidungsansätze zielen auf den Verzicht risikoreicher Geschäfte ab und streben daher eine vollständige Eliminierung der Risikoursache an. Allerdings gilt es zu erwähnen, dass dieses Konzept keine Anwendung bei symmetrischen Unsicherheiten darstellt, da folglich auf jegliche Chancen verzichtet wird und das Sicherheitsziel konsequent über andere Unternehmensziele (zum Beispiel Gewinnziele) gestellt wird (vgl. Pfohl et al.

2008a, S. 67). Das zentrale Ziel der Risikovermeidung besteht darin, ungeachtet vom möglichen Schadenausmaß, die Eintrittswahrscheinlichkeit der Risikoursache zu beseitigen. Bei Risiken, die ihren Ursprung außerhalb des einzelnen Unternehmens haben, erscheint eine effektive Steuerung anhand von Risikovermeidungsstrategien allerdings zweifelhaft (vgl. Grotegut 2006, S. 39 f.). Dennoch kann die Vermeidung risikobehafteter Aktivitäten in diversen Entscheidungsszenarien aus Sicht der Lieferkette tatsächlich eine sinnvolle Handlungsalternative darstellen. Als Beispiel lässt sich hierbei die Aufnahme einer neuen Produktart in das Angebot der Lieferkette aufführen. Auch der Austritt einzelner Partner aus der Supply-Chain sowie der Verzicht auf bestimmte Leistungen der Lieferkette lassen sich als mögliche Risikovermeidungsmaßnahmen anführen (vgl. Götze und Mikus 2015, S. 49).

Insgesamt lässt sich feststellen, dass Maßnahmen zur vollständigen Eliminierung der Risiken nicht auf alle Formen von Risikoursachen anwendbar sind. Vor allem Naturkatastrophen oder andere Katastropheneignisse sind in den meisten Fällen nur schwierig oder überhaupt nicht steuerbar. In diesen Fällen muss auf Lösungsansätze der wirkungsbezogenen Steuerungsmaßnahmen ausgewichen werden (vgl. Wagner und Bode 2007, S. 69). Eine alternative Herangehensweise zur Reduzierung der Risikoquellen für Naturereignisse ist die Auswahl eines Lieferanten in einem nicht exponierten Gebiet. Vor allem bei Naturgefahrenexponierung und Single-Source-Lieferanten stellt dies die einzige Möglichkeit dar, eine Betriebsunterbrechung zu vermeiden.

Risikoverminderung

Praktisch von wesentlich größerer Relevanz sind die Maßnahmen zur Risikoverminderung. Hierzu eignen insbesondere organisatorische Maßnahmen und Kontrollen, die sich durch die Verminderung der Gefahr menschlichen Versagens auszeichnen, sowie Sicherungsmaßnahmen wie präventive Qualitätskontrollen, regelmäßige Instandhaltungsarbeiten bei Produktionsmaschinen und das Ersetzen von Gefahrstoffen (vgl. Mikus 2001, S. 177). Ferner sind zudem Konzepte zur Planungsgestaltung, die einen Umgang mit Unsicherheiten bezüglich der Endnachfrage gewährleisten, als weitere Handlungsmaßnahmen in der genannten Kategorie aufzuführen (vgl. Mikus 2001, S. 226).

In Bezug auf die endogenen Risiken der Lieferkette lässt sich die risikobezogene Auswahl geeigneter Kooperationspartner entlang der Supply-Chain der Risikoverminderung zuordnen. So wird versucht, eine Bindung zu einem Lieferanten anzustreben, der eine besondere Lieferzuverlässigkeit aufweist, um das Risiko in der Beschaffung zu minimieren. Zu Verminderung von finanziellen Risiken erscheint zum Beispiel die Auswahl der Kooperationsakteure hinsichtlich ihrer finanziellen Situation als sinnvoll (vgl. Götze und Mikus 2015, S. 47). Ebenso lassen sich durch eine offene risikoorientierte Kommunikation zwischen den Partnern der Supply-Chain Risiken reduzieren. Als Beispiel lässt sich das Open-Book-Accounting aufführen, bei dem monetäre und nicht-monetäre Informationen unternehmensübergreifend jederzeit zur Verfügung stehen (vgl. Pfohl et al. 2008a, S. 67).

Als weiteren Ansatz zur effektiven Reduzierung der Eintrittswahrscheinlichkeit von Supply-Chain-bezogenen Risikoereignissen lässt sich die Entwicklung einer unternehmensübergreifenden Risikokultur innerhalb der Supply-Chain anführen. Hierbei gilt als Voraussetzung, eine gemeinsame bewusste Handhabung mit potenziellen Risiken über alle Partner hinweg zu integrieren (vgl. Götze und Mikus 2015, S. 47).

25.3.3.2 Wirkungsbezogene Steuerungsmaßnahmen

Wirkungsbezogene Steuerungsansätze stellen Handlungsmaßnahmen dar, die auf eine Verbesserung des Ergebnisses im Falle des Risikoeintrittes abzielen. Sie dienen vor allem dazu, drohende Schäden bzw. Verluste zu reduzieren, begrenzen oder zu kompensieren (vgl. Mikus 2001, S. 178). Im Einzelnen lassen sich hierunter die Risikobegrenzung und -übertragung, Risikoteilung sowie Risikoselbsttragung einordnen (vgl. Pfohl et al. 2008a, S. 68).

Risikobegrenzung und Risikotransfer

Risikobegrenzung und -transfer lassen sich generell durch entsprechende Vereinbarungen mit anderen Unternehmen darstellen. Dies kann neben dem Abschluss von Versicherungen, der Vereinbarung von bestimmten Vertragsklauseln oder Haftungsregelungen mit Vertragspartnern erfolgen. Die Maßnahmen dabei können sowohl auf endogene sowie auf exogene Risiken gerichtet sein. Bezogen auf die Lieferkette sind verschiedene Möglichkeiten der Risikobegrenzung und -übertragung existent. Zum einen kann eine Risikobegrenzung in einzelnen Supply-Chain-Unternehmen eine Verbesserung der Zielerreichung der gesamten Lieferkette hervorrufen, indem Lieferanten bzw. Zulieferer Risiken auf Unternehmen übertragen, die sich außerhalb des Liefernetzwerkes befinden. Zum anderen kann eine Risikoübertragung innerhalb der Lieferkette bestehen, die durch das Ausnutzen der Risikopräferenz und -tragfähigkeit der einzelnen Partner die Risikosituation bzw. das Gesamtresultat tendenziell optimiert. Dies kann zum Beispiel im Zuge einer Abnahmeverpflichtung erfolgen, mit der ein Unternehmen das Absatzrisiko eines Supply-Chain Akteurs vermindert (vgl. Götze und Mikus 2015, S. 50).

Der Kauf von Versicherungslösungen stellt für Unternehmen ein Instrument der Risikosteuerung dar, mit dem im Rahmen des Risikomanagements Risiken an Versicherungsgesellschaften transferiert werden können. Durch den Abschluss von Versicherungen werden vor allem Aufwendungen der Unternehmen bei unerwarteten Schadeneignissen verringert. Zugleich kommt es durch den Transfer des Risikos zu einer Erhöhung der Planungssicherheit. Die grundlegende Basis für den Einsatz von Versicherungen als risikopolitische Steuerungsmaßnahme stellt die Prüfung der Versicherbarkeit von Risiken mithilfe eines mehrstufigen Problemlösungsprozesses dar. Zur Absicherung der vielschichtigen Risiken und Gefahren bestehen im Rahmen von Logistikprozessen unterschiedliche Versicherungsprodukte. Für den Schutz der physischen Transportprozesse und der damit einhergehenden Risiken eignet sich eine Transportversicherung. Zur Kompensation eines Ausfalls der Betriebsaktivität dient die Betriebsunterbrechungsversicherung (vgl. Skorna 2016, S. 211 ff.).

Die Transportversicherung beinhaltet im Leistungsumfang grundsätzlich die Gefahrenabdeckung für bewegte Transportgüter und Transportmittel (vgl. Robold 2010, S. 212). Neben der Möglichkeit zur Absicherung gegen Beschädigungen und den Verlust von Gütern lässt sich in der Transportversicherung ebenso die Betriebsunterbrechung infolge eines versicherten Ereignisses absichern. Voraussetzung dabei ist, dass die Lieferkomplikationen als unmittelbare Folge auf einen versicherten Güterschaden resultieren. „Ein Güterfolgeschaden liegt [dann] vor, wenn die Verwendung der versicherten Güter infolge eines ... [versicherten] Schadens beeinträchtigt oder nicht mehr möglich ist und dadurch ... [die] fortlaufenden Kosten zur Fortführung des Unternehmens nicht erwirtschaftet werden konnten. Kosten werden nur ersetzt, soweit ihr Weiteraufwand rechtlich notwendig oder wirtschaftlich begründet ist“ (GDV 2011). Risiken bzw. Gefahren, die sich außerhalb des physischen Transports befinden, lassen sich über die Transportversicherung allerdings nur beschränkt abdecken. Aus diesem Grund basieren die Diskussionen für die Absicherung von Risiken einer Supply-Chain auf Konzepten der Sachversicherung. Insofern bedarf es eine kurze Erläuterung über Ansätze der Betriebsunterbrechungsversicherung (vgl. Skorna 2016, S. 215).

Die Betriebsunterbrechungsversicherung (BU-Versicherung) stellt heute die allgemein üblichste Form der Ertragsausfalldeckung dar. Detailliert betrachtet ist sie der Vermögensversicherung zuzuordnen. Der Versicherungsvertrag ist an dem allgemeinen Unternehmensziel der Gewinnmaximierung ausgerichtet und umfasst die Deckung eines Betriebsunterbrechungsschadens. Dieser wird bestimmt durch den während der Haftzeit entgangenen Betriebsgewinn sowie den Aufwand an fortlaufenden Kosten, die aufgrund der Unterbrechung nicht erwirtschaftet werden konnten, ohne Eintritt des versicherten Ereignisses jedoch erwirtschaftet worden wären. In der traditionellen Auslegung ist die Deckungsvoraussetzung der Eintritt eines versicherten Sachschadens, der zur Betriebsunterbrechung führt (vgl. Lange und Robold 2010, S. 198 f.; vgl. Skorna 2016, S. 215). Eine Besonderheit in der BU-Versicherung stellen die sogenannten Wechselwirkungsschäden dar. Diese bezeichnen die Auswirkungen eines Sachschadens in einer Betriebsstelle auf andere Betriebsstellen desselben Unternehmens. Voraussetzung hierbei ist, dass die Absicherung des gesamten Betriebes in einem Vertrag zusammengefasst ist. Zudem muss sich der ersatzpflichtige Schaden, der eine Betriebsunterbrechung auslöst, an einem dieser Betriebsstandorte ereignen (vgl. Skorna 2016, S. 215). Die originäre BU-Versicherung umfasst die Deckung innerbetrieblicher Produktionsprozesse, erstreckt sich jedoch nicht auf einen Schutz für Lieferkettenrisiken. Für betriebsfremde, ausgelagerte Produktionsprozesse ist eine erweiterte BU-Versicherung mit Rückwirkungsschadenklausel notwendig. Dadurch wird die Deckung (meist limitiert) erweitert auf Betriebsunterbrechungsschäden, deren Ursprung in einem Sachschaden bei einem Zulieferer oder Abnehmer liegt. Voraussetzung dabei ist, dass der Sachsachen gedeckt gewesen wäre, wenn er beim versicherten Unternehmen eingetreten wäre (vgl. Zimmer 2017, S. 2).

In der Literatur wird im Rahmen der Optimierung von Supply-Chain-bezogenen Risiken ebenso die Gründung von Captives vorgeschlagen. Captives (Captive (Re) Insurance Undertakings) stellen Erst- oder Rückversicherer dar, die einem Industrie-, Handels- oder

Finanzunternehmen angehören, welche selbst allerdings kein Versicherungsgeschäft betreiben. In erster Linie konzentrieren sie sich auf die Absicherung interner Risiken. Erstversicherungs-Captives sind dabei auf die direkte Deckung von Konzernrisiken ausgelegt. Rückversicherungs-Captives hingegen indirekt einen im Rückversicherungsvertrag definierten Teil des Risikos von einem zugelassenen Erstversicherer (vgl. BaFin 2017). Captives bieten daher die Möglichkeit, auch schwer versicherbare Risiken auf eine Versicherung zu transferieren und damit die Grenzen der Versicherbarkeit auszuweiten. Die Zielsetzung lässt sich hinsichtlich folgender Punkte unterscheiden: Partizipation am eigenen Schadenverlauf, Kostengründe sowie Versicherung nicht versicherbarer Risiken. Im Zuge des Risikomanagements in Supply-Chains existiert daher die Überlegung, dass sich eine Vielzahl von Unternehmen zusammenschließen und eine solche Captive-Lösung gründen, um sich somit gegen endogene Supply-Chain Risiken abzusichern (vgl. Pfohl et al. 2008a, S. 69).

Risikoteilung

Eine weitere Möglichkeit zum wirkungsbezogenen Agieren ist die Risikoteilung. Hierbei wird eine Risikoverminderung angestrebt, indem unternehmerische Aktivitäten in mehrere Teilaktivitäten zerlegt werden. Sie bietet sich vor allem für die risikopolitische Steuerung im Rahmen des Supply-Chain-Managements an, da für dieses die bewusste Allokation von Prozessen der Leistungserstellung auf Akteure der Lieferkette charakteristisch ist und mit der Supply-Chain-Bildung auch das Ziel der Aufsplittung von Risiken fokussiert werden kann (vgl. Götze und Mikus 2015, S. 50).

Eine Aufteilung des Risikos kann insbesondere durch eine entsprechende Konfiguration und Koordination des Supply-Chain-Netzwerks erfolgen. Dies wirkt sich unmittelbar auf die Gestaltung der Lieferanten-, Produktionsstätten- und Lagerstruktur aus (vgl. Mikus 2001, S. 225). Die Konfiguration legt dabei den langfristig anerkannten Rahmen fest, innerhalb dessen sich koordinierenden Tätigkeiten realisieren können. Dadurch wird zwar einerseits eine schnelle Reaktion sichergestellt, diese wird aber andererseits durch die vorher bestimmte Struktur beschränkt (vgl. Pfohl et al. 2008a, S. 69).

Die Grundidee der Risikoteilung besteht darin, neben den primär genutzten Lieferantenverbindungen, Produktionsstätten und Lagerorten weitere ungebundene Verbindungen zu anderen Standorten zu pflegen, um bei einem Ausfall der Hauptbeziehung auf alternative Bezugsquellen ausweichen zu können (vgl. Delfmann und Albers 2000, S. 57). Folglich muss gelten, dass der entsprechende Standort über die nötige Ausstattung, erforderliche Kapazitäten sowie die Bereitschaft zur Übernahme der Tätigkeiten verfügt (vgl. Sheffi 2001, S. 2). Eine konkrete Umsetzung der Risikoteilung ist dabei der kurzfristige Rückgriff auf sekundäre Lieferantenquellen. Hierbei wird vor allem beim Global Sourcing Abhilfe geschaffen, wenn zusätzliche regional angesiedelte Bezugsquellen mit kurzen Lieferzeiten eingebunden werden, auf die in einer Notbedarfslage zurückgegriffen werden kann (vgl. Melzer-Ridinger 2001b, S. 50). Die daraus resultierenden zusätzlichen Kosten sind implizit als Versicherungsprämien aufzufassen, die das Lieferrisiko unter Akzeptanz von gestiegenen Beschaffungspreisen reduzieren (vgl. Sheffi 2001, S. 3). Ferner ist ausge-

hend von einer bestehenden Supply-Chain-Struktur eine weitere explizite Risikoteilung in Form von einer räumlichen und/oder zeitlichen Zerlegung der Wertschöpfungsaktivitäten möglich. Als Beispiel lässt sich hierbei die Nutzung von zusätzlichen dezentralen Lagern aufführen (vgl. Götze und Mikus 2015, S. 50).

Risikoselbsttragung

Zur abschließenden Betrachtung der wirkungsbezogenen Steuerungsmaßnahmen wird im Folgenden die Risikoselbsttragung beschrieben. Wird eine solcher Ansatz innerhalb der Supply-Chain gewählt, so bedeutet dies, dass die Auswirkungen eines Risikoeintritts zwar bewusst getragen, aber in der Regel entsprechende Maßnahmen eingeleitet werden, um dennoch die Zielerreichung sicherzustellen (vgl. Götze und Mikus 2015, S. 51). Die Eigentragung von Risiken ist ein wesentlicher Teil eines jeden Risikomanagementprozesses. In jedem Einzelfall ist zu klären, wie viel Risiko ein Unternehmen tragen kann (Finanzkraft) und wie viel Risiko die Unternehmensführung bereit ist einzugehen (Risikoaversion). Nur der Teil des Gesamtrisikos, der nach Vermeidung und Verminderung verbleibt, jedoch aus finanziellen Gründen nicht tragbar wäre, oder aufgrund der individuellen Risikoaversion der Entscheidungsträger nicht akzeptiert wird, ist zu transferieren. Keinerlei Risiko selbst zu tragen (vergleichbar mit einer Versicherung ohne Selbstbehalt) ist zumindest bei industriellen Großrisiken keine effiziente Art, ein Risiko abzusichern, und aufgrund von limitierten Deckungen und Kapazitätsbeschränkungen des Versicherungsmarktes meist nicht möglich.

Aus Risikosicht lassen sich damit bestimmte Maßnahmen aufführen, die das Schadensausmaß bei Eintritt der Risikoursachen möglichst gering halten sollen. Diese gewissen Redundanzen können sich auf verschiedene Bereiche im Unternehmen beziehen (vgl. Pfohl et al. 2008a, S. 70).

Hierzu zählt zum Beispiel eine Verlustdeckung, die durch die Bildung von finanziellen, güterbezogenen und personellen Reserven entsteht. Dies kann über die Bildung von Rückstellungen und Rücklagen, die Berücksichtigung kalkulatorischer Wagniskosten, das Vorhalten von Aushilfspersonal bei einzelnen Unternehmen der Lieferkette, entsprechende Eingangs- und Zwischenlagerbestände sowie durch die Einplanung von Pufferzeiten zwischen den einzelnen Supply-Chain-Akteuren erfolgen. Des Weiteren werden gewisse Maßnahmen vorgeschlagen, die zur allgemeinen Erhöhung der Flexibilisierung von einzelnen Supply-Chain-Mitgliedern oder der Lieferkette selbst beitragen. Dieser Prozess wird unterstützt durch die Integration flexibler Produktionskonzepte, den Einsatz universeller -bzw. von Mehrzweckmaschinen, der Weiterbildung der Mitarbeiter, der Nutzung von leicht zu ersetzendem Material, durch flexible Prozessgestaltung- und -steuerung (dies kann zum Beispiel über variierbare Reihenfolge- und Terminpläne sichergestellt werden) sowie durch eine anpassungsfähige Beschaffungs- und Lagerhaltungsplanung (vgl. Götze und Mikus 2015, S. 51).

Eine Zusammenfassung verschiedener risikobezogener Maßnahmen zu einem Maßnahmenbündel kann nicht nur auf Unternehmensebene, sondern auch im Rahmen der gesamten Lieferkette praktiziert werden, um die Herausforderungen der komplexen Umwelt

sowie die vielschichtigen Interdependenzen zu bewältigen. Bei einem solchen Maßnahmenbündel spricht man von dem Ansatz der resilienten Supply-Chain (vgl. Pfohl et al. 2008a, S. 70). Es erfolgt dabei eine Zusammenfassung bestimmter Maßnahmen, wie der Erstellung eines gemeinsamen Risikokatalogs, der Erhöhung der Transparenz und kooperierender Planungsaktivitäten, der Entwicklung einer simultanen Risikokultur innerhalb der Supply-Chain sowie ein umfassendes Lieferantenmanagement – vorausgesetzt sie werden in den einzelnen Unternehmen sowie der Lieferkette geschlossen umgesetzt. Das zentrale Ziel dabei besteht darin, die Widerstandsfähigkeit der Supply-Chain bei einer Störung gezielt zu stärken (vgl. Christopher und Peck 2004, S. 6 ff.).

25.3.3.3 IT-gestütztes Supply-Chain-Risikomanagement anhand eines Beispiels der Continental AG

In Zeiten der digitalen Transformation mit ihren Entwicklungstreibern wie Big Data und Data Analytics existieren Tools, die den gesamten Risikomanagementprozess unterstützen oder sogar übernehmen können (vgl. Zimmer 2017). Mithilfe einer prozessgestützten Cloudlösung hat die Continental AG ein ganzheitliches und modernes Supply-Chain-Konzept für das Risiko- und Allokationsmanagement entwickelt, das basierend auf intelligenten Algorithmen Echtzeit-Analysen der Lieferketten ermöglicht und unterstützt. Damit wird eine kontinuierliche, digitale Überwachung von Kapazitätsrisiken in Zusammenarbeit mit den Lieferanten sichergestellt. Für das Projekt wurde die Continental AG mit dem Logistik-Award 2019 des Verbands der Automobilindustrie ausgezeichnet (vgl. Rotter 2019).

Zielsetzung

Im Rahmen des Projektes „Continental Supply Risk Management 4.0“ werden zwei konkrete Ziele verfolgt. Zum einen soll eine signifikante Reduzierung der Vorlaufzeit bis zur Information des Endkunden im Falle eines möglichen Rohstoffrisikos erfolgen. Die Rückmeldung an den Kunden über einen drohenden Lieferengpass soll von 48 auf zwölf Stunden reduziert werden. Dabei ist die Berechnung der Endkundenreichweite unter Berücksichtigung sämtlicher Kundenbedarfe und Materialbeziehungen zu standardisieren und entlang der Lieferkette zu simulieren. Das zweite Ziel umfasst den Aufbau eines ganzheitlichen Lieferanten-Risikomanagements durch die Ergänzung der bestehenden Prozesse in Form einer kontinuierlichen Risikoanalyse der Supply-Chain (Risikoprävention). Die Umsetzung der beiden genannten Ziele folgt der Vision, die Lieferkette zu digitalisieren und ein Netzwerk aus allen beteiligten Partnern aufzubauen (vgl. Continental AG 2019).

Beschreibung des Projektes

Zur Erreichung der aufgeführten Ziele wurden drei auf einander abgestimmte Teilprojekte zusammengeführt: Es erfolgte die Entwicklung eines ganzheitlichen Ansatzes, das unternehmensinterne Material Shortage Management 12h (MSM12h), das Supplier Capacity Update (SCU) sowie das Vendor Information Portal (VIP) in ein Konzept zu integrieren.

Das VIP ist eine einheitliche und datentechnisch voll-integrierte Schnittstelle zwischen der Continental AG und ihren Lieferanten. Das VIP stellt damit die Voraussetzung für das MSM12h und SCU dar, indem es die benötigten Informationen harmonisiert und verbindet. Das MSM12h ist ein Problemlösungsansatz im kurzfristigen Bereich, der bei Naturkatastrophen und lokalen Ereignissen zum Tragen kommt. Es bildet die Voraussetzung für die erforderlichen Prozesse und IT-Strukturen, um Kunden im Falle eines signifikanten Supply-Chain-Risikos mit möglicher Auswirkung auf Continental-Lieferanten darüber zu benachrichtigen, ob ihre Projekte betroffen sind oder nicht. Das SCU beinhaltet einen kontinuierlichen Soll-Ist-Abgleich zwischen vereinbarten Liefermengen, tatsächlichen Materialabrufen sowie den (künftig) zur Verfügung stehenden Kapazitäten der Lieferanten. Es stellt damit einen Prozess dar, der bereits im Vorfeld potenzielle Engpässe erkennt. Wie eingangs beschrieben, können verschiedene Ursachen eine Betriebsunterbrechung in der Lieferkette hervorrufen. Von der Continental AG wurden hierbei vor allem Probleme bei der Kapazitätsplanung, veränderte Marktsituationen, drohende Naturkatastrophen sowie Standort-Vorfälle als Haupttreiber der Herausforderung hervorgehoben (vgl. Continental AG 2019).

Das MSM12h, der Nukleus der Innovation der Continental AG, wurde intensiv optimiert. In der Vergangenheit betrug der Prozess oftmals bis zu einer Woche, um in deren Systemen, Nomenklaturen sowie Datensätzen das Rohmaterial den Kunden-/Endprodukten zuzuordnen, um eine Aussage darüber treffen zu können, welches bestimmte Teil betroffen ist und welche Reichweiten diese in deren Werken durch Bestände und Vororte etc. haben. Dies ist die Grundlage, um letztlich zu bestimmen, wann ein erster möglicher Produktionsausfall bzw. eine erste Nichtbelieferung der Kunden eintreten wird. Dieser Prozess wurde durch das Zusammenführen in ein System, mit der Einführung von Algorithmen und dem damit verbundenen Wegfall aller manuellen, sich oftmals wiederholenden Tätigkeiten von ursprünglich 48 auf zwölf Stunden reduziert (vgl. Continental AG 2019).

Beziehung zwischen den drei Teilprojekten

Die drei Teilprojekte (VIP, MSM12h, SCU) sind eng miteinander verzahnt und als Bestandteile eines ganzheitlichen Logistikkonzepts zur Reduzierung des Versorgungsrisikos entlang der Wertschöpfungskette (Risiko-Prävention und Problembehandlung) sowie zur Digitalisierung der Supply-Chain zu sehen. Das VIP fungiert als „Enabler“, der die Voraussetzung für einen kontinuierlichen und standardisierten Informationsaustausch zwischen der Continental AG und ihren Lieferanten schafft. Das Zusammenspiel der drei Teilprojekte begünstigt mehrere Prozessverbesserungen. Eine Risikoprävention (insbesondere im Rahmen von SCU) wird erreicht durch neue Prozesse, fortschrittliche Ansätze, Methoden aus dem Bereich Data Analytics (unter anderem Data Mining) sowie dem Einsatz von Big Data- und Cloud-Technologien. Im Detail werden in einem neu geschaffenen Supply-Chain-Monitor Echtzeit-Analysen und eine kontinuierliche Überwachung von Kapazitätsrisiken durchgeführt. Zudem stellt die Integration von Lieferanten- und Kundeninformationen in einer gemeinsamen Datenbank notwendige Informationen kontinuierlich zur Verfügung. Die auf Werks-Ebene durchgeführte individuelle und manuelle Be-



Abb. 25.2 Continental Supply Risk Management 4.0. (Quelle: eigene Darstellung in Anlehnung an Continental AG 2019)

rechnung der Endkundenreichweite wird durch eine globale Simulation abgelöst. Dadurch wird eine Verkürzung der Vorlaufzeit zur Kundeninformation von 48 Stunden auf nunmehr zwölf Stunden ermöglicht (vgl. Continental 2019) (Abb. 25.2).

Insgesamt ist es der Continental AG gelungen, ein ganzheitliches und transparentes Risikomanagement-Tool zu entwickeln, das durch die Digitalisierung eine Vernetzung der gesamten Wertschöpfungskette herbeiführt, neue Wege der Risikoprävention und Problembehandlung ermöglicht und gleichzeitig durch eine Supply-Chain-weite Datenharmonisierung eine Reduzierung nicht wertschöpfender Tätigkeiten schafft (vgl. Continental AG 2019).

25.4 Fazit

Im Zuge der zunehmenden Globalisierung und Reduzierung der Wertschöpfungstiefe findet man fortschrittliche und komplexe Lieferketten vor, die eine ausgeprägte Fragmentierung und eine damit verbundene Verletzlichkeit der Supply-Chain aufweisen. Die Folge ist ein neues Maß an Unsicherheit und Risiko. Zur Sicherung der Wettbewerbsfähigkeit der einzelnen Unternehmen nimmt die Bedeutung des Risikomanagements für Supply-Chain-bezogene Risiken eine neue Dimension an. Ausgehend von den unternehmensintern ausgerichteten Risikomanagementprozessen ist ein entsprechendes Konzept zu entwickeln, das sich auf die Steuerung der gesamten Supply-Chain übertragen lässt. Eine gemeinsame Identifizierung, Analyse und Bewertung sowie ein einheitliches Verständnis über Risiken bilden die entscheidende Grundlage für die Risikopolitik, um das Konzept in allen beteiligten Handels-, Industrie- und Dienstleistungsunternehmen wirksam zu implementieren (vgl. Pfohl et al. 2008a, S. 79). Bei der Herangehensweise des Risikomanagements in der Supply-Chain lassen sich verschiedene konzeptionelle Ansätze unterscheiden. Während ein Risikomanagement mit Supply-Chain-Orientierung gänzlich eine unternehmensin-

terne Ausrichtung bietet, besteht bei den gemeinsamen Risikoanalysen innerhalb der Lieferkette oder beim Supply-Chain-Risikomanagement die Möglichkeit, durch eine unternehmensübergreifende Zusammenarbeit die Identifizierung und risikopolitische Steuerung von Risiken zu verbessern und eine höhere Transparenz über die Risikosituation in der Supply-Chain anzustreben. Ein unternehmensübergreifendes Risikomanagement wird primär in Form eines Risikomanagements mit Supply-Chain-Orientierung oder vereinzelt in Form von gemeinsamen Risikoanalysen praktiziert. Ein integriertes Supply-Chain-Risikomanagement, wie es eingangs beschrieben wurde, existiert in der Praxis nur selten (vgl. Kajüter 2015, S. 24).

Beim Risikomanagement in einer Lieferkette besteht zusätzlich die Besonderheit, dass die Interessen der verschiedenen Akteure bei der risikobezogenen Zielsetzung berücksichtigt werden müssen. Ausgehend von den unterschiedlichen Risikopräferenzen und Risikotragfähigkeiten sollten zunächst die risikobezogenen Zielsetzungen der einzelnen Akteure – gegliedert nach den vier aufgeführten Ebenen – und deren damit zusammenhängende Risikotragfähigkeit erfasst werden, um den Abstimmungsbedarf zu konkretisieren. Im Ergebnis hierbei wird ersichtlich, dass ein risikobezogenes Zielsystem einer Lieferkette gebildet werden sollte, das zu den Sicherheitsbedürfnisse der einzelnen Supply-Chain-Partner passt und ferner Sicherheitsziele umfassen kann, die lediglich aus Sicht einzelner Unternehmen erforderlich sind (vgl. Götze und Mikus 2015, S. 31 ff.).

Studien zeigen, dass der Grad der Professionalisierung des Risikomanagements weder mit der Branche des Unternehmens noch mit dessen Größe korreliert. Auch wenn in dem vorliegenden Beitrag nicht alle denkbaren Faktoren berücksichtigt wurden, legen die Befunde nahe, dass Risikomanagement in der Supply-Chain ein Thema darstellt, das durch individuelles Risikobewusstsein des Managements getrieben wird. Steigt die Fragmentierung der Lieferketten weiterhin an, und zwar in einer Umwelt, die von stetiger Dynamik und Unsicherheit geprägt ist, so wird dem Management von Supply-Chain-Risiken ebenso eine erhöhte Aufmerksamkeit zuzuschreiben sein (vgl. Börner und Armon 2015).

Literatur

- BaFin. (2017). *Captives: BaFin lädt konzerneigene Versicherungsunternehmen zum Austausch.* https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2017/fa_bj_1704_Captives.html vom 15.04.2017. Zugegriffen am 30.05.2019.
- Bayer, F., & Bioly, S. (2014). *Supply Chain Risk Management in der Industrie – am Beispiel der Metall- und Elektroindustrie.* Essen: Akademie Verlags- und Druck-Gesellschaft mbH.
- Börner, C. J., & Armon, M. (2015). Risikomanagement in der Supply Chain - Herausforderungen und Lösungen. *Die Versicherungspraxis* (2).
- Buchhart, A., & Burger, A. (2001). *Risiko-Controlling.* Berlin: De Gruyter Oldenbourg.
- Christopher, M., & Lee, H. (2004). Mitigating supply chain risk through improved confidence. *International Journal of Physical Distribution & Logistics Management*, 5, 388–396.
- Christopher, M., & Peck, H. (2004). Building the resilient supply chain. *International Journal of Logistics Management*, 2, 1–13.
- Continental AG. (2019). Supply Risk Management 4.0. VDA Logistik Award 2019.

- Cuccheilla, F., & Gastaldi, M. (2006). Risk management in supply chain: A real option approach. *Journal of manufacturing technology*, 6, 700–720.
- Delfmann, W., & Albers, S. (2000). Supply Chain Management in the global context: Arbeitsbericht Nr. 102 des Seminars Allgemeine Betriebswirtschaftslehre, betriebswirtschaftliche Planung und Logistik der Universität Köln. Köln.
- Etterer, W. (2008). In H.-C. Pfohl (Hrsg.), *Handlungsstrategien im Risikomanagement für kleine und mittlere Unternehmen aus Sicht eines mittelständischen Logistikdienstleisters*, in *Sicherheit und Risikomanagement in der Supply Chain: Gestaltungsansätze und praktische Umsetzung* (S. 193–214). Hamburg: DVV-Media-Group Dt. Verkehrsverlag.
- Fiege, S. (2006). *Risikomanagement- und Überwachungssystem nach KonTraG: Prozess, Instrumente, Träger*. Wiesbaden: DUV Deutscher Universitätsverlag.
- Gabath, C. (2010). *Risiko- und Krisenmanagement im Einkauf: Methoden zur aktiven Kostensenkung*. Wiesbaden: Gabler/Springer Fachmedien.
- GDV. (2011). DTV-Gütersicherungsbedingungen 2000/2011. Güterfolgeschadenklausel. Musterbedingungen des GDV.
- Giunipero, L. C., & Eltantawy, R. A. (2004). Securing the upstream supply chain: A Risk Management approach. *International Journal of Physical Distribution & Logistics Management*, 9, 698–713.
- Göpfert, I., Grünert, M., & Schmid, N. A. (2016). Logistiknetze der Zukunft – Das neue Hersteller-Zulieferer-Verhältnis in der Automobilindustrie. In I. Göpfert (Hrsg.), *Logistik der Zukunft - Logistics for the Future* (S. 175–218). Wiesbaden: Springer Gabler.
- Götze, U., & Mikus, B. (2015). Der Prozess des Risikomanagements in Supply Chains. In C. Siepermann, R. Vahrenkamp & M. Siepermann (Hrsg.), *Risikomanagement in Supply Chains: Gefahren abwehren, Chancen nutzen, Erfolg generieren* (S. 29–62). Berlin: Erich Schmidt.
- Grotzegut, M. (2006). *Risiken im Einkauf: Ihre Analyse, Bewertung und Behandlung unter besonderer Berücksichtigung ökonomischer und rechtlicher Aspekte*. Zugl.: Duisburg, Essen, Univ., Diplomarbeit, 2004. München: GRIN.
- Harland, C., Brenchley, R., & Walker, H. (2003). Risk in supply networks. *Journal of Purchasing & Supply Management*, 2, 51–62.
- Horvath, P., & Gleich, R. (2000). Controlling als Teil des Risikomanagements. In D. Dörner (Hrsg.), *Praxis des Risikomanagements: Grundlagen, Kategorien, branchenspezifische und strukturelle Aspekte* (S. 100–126). Stuttgart: Schäffer-Poeschel.
- Jung, K.-P., & Nowitzky, I. (2006). Das besondere Risikopotenzial in der Logistik. In G. Blaas & B. Hector (Hrsg.), *Riskmanagement in der Logistik* (S. 61–69). Hamburg: Dt. Verkehrsverlag.
- Jüttner, U., Peck, H., & Christopher, M. (2003). Supply chain risk management: Outlining an agenda for future research. *International Journal of Logistics: Research and Applications*, 4, 197–210.
- Jüttner, U., & Ziegenbein, A. (2009). Supply chain risk management for small and medium-sized businesses. In G. A. Zsidisin and B. Ritchie (Hrsg.), *Supply chain risk: A handbook of assessment, management, and performance* (S. 199–217). Boston, MA: Springer.
- Kajüter, P. (2003). Instrumente Zum Risikomanagement in der Supply Chain. In W. Stölzle & A. Otto (Hrsg.), *Supply Chain Controlling in Theorie und Praxis: Aktuelle Konzepte und Unternehmensbeispiele* (S. 107–135). Wiesbaden: Gabler.
- Kajüter, P. (2015). Risikomanagement in der Supply Chain: Ökonomische, regulatorische und konzeptionelle Grundlagen. In C. Siepermann, R. Vahrenkamp & M. Siepermann (Hrsg.), *Risikomanagement in Supply Chains: Gefahren abwehren, Chancen nutzen, Erfolg generieren* (S. 13–28). Berlin: Erich Schmidt.
- Kersten, W., Böger, M., Hohrath, P., & Späth, H. (2006a). Supply chain risk management: Development of a theoretical and empirical framework. In W. Kersten (Hrsg.), *Managing risks in supply chains: How to build reliable collaboration in logistics* (S. 3–18). Bremen: Erich Schmidt.

- Kersten, W., Hohrath, P., Böger, M., & Späth, H. (2006b). Wissensmanagement als Instrument des Supply Chain Risk Managements. In H.-C. Pfohl (Hrsg.), *Wissenschaft und Praxis im Dialog: Steuerung von Logistiksystemen - auf dem Weg zur Selbststeuerung; [3. Wissenschaftssymposium Logistik in Dortmund]* (S. 233–269). Hamburg: Dt. Verkehrsverlag.
- Kaye, D. 2008. *Managing risk and resilience in the supply chain*. London: BSI Business Information.
- Lange, M., & Robold, M. (2010). Kriterien der Produktgestaltung unter Berücksichtigung von rechtlichen und kalkulatorischen Rahmenbedingungen. In M. Lange & M. Robold (Hrsg.), *Sachversicherungen für private und gewerbliche Kunden: Fach- und Führungskompetenz für die Assekuranz; geprüfter Fachwirt für Versicherungen und Finanzen, geprüfte Fachwirtin für Versicherungen und Finanzen* (S. 53–211). Karlsruhe: VVW.
- Lasch, R., Janker, C. G., & Derno, M. (2015). Risikoorientiertes Lieferantenmanagement. In C. Siepermann, R. Vahrenkamp & M. Siepermann (Hrsg.), *Risikomanagement in Supply Chains: Gefahren abwehren, Chancen nutzen, Erfolg generieren* (S. 77–102). Berlin: Erich Schmidt.
- Melzer-Ridinger, R. (2001a). Risikoarten richtig gewichten (I), Systematisches und umfassendes Risikomanagement. *Beschaffung Aktuell*, 1, 45–46.
- Melzer-Ridinger, R. (2001b). Risikoarten richtig gewichten (II), Bewältigung des Fehlmengenrisikos. *Beschaffung Aktuell*, 2, 48–51.
- Mikus, B. (2001). *Make-or-buy-Entscheidungen: Führungsprozesse, Risikomanagement und Modelanalysen*. Zugl.: Göttingen, Univ., Diss, 1997 u.d.T.: Mikus, Barbara: Make-or-buy-Entscheidungen in der Produktion. Chemnitz: GUC.
- Mikus, B. (2003). *Strategisches Logistikmanagement: Ein markt-, prozess- und ressourcenorientiertes Konzept*. Wiesbaden: Deutscher Universitätsverlag.
- Mikus, B. (2009). *Make-or-buy-Entscheidungen: Führungsprozesse, Risikomanagement und Modelanalysen*. Zugl.: Göttingen, Univ., Diss., 1997 u.d.T.: Mikus, Barbara : Make-or-buy-Entscheidungen in der Produktion. Chemnitz: GUC - Verl. der Ges. für Unternehmensrechnung und Controlling.
- Norrman, A., & Jansson, U. (2004). Ericsson proactive supply chain risk management approach after a serious sub-supplier accident. *International Journal of Physical Distribution & Logistics Management*, 5, 434–456.
- Norrman, A., & Lindroth, R. (2004). Categorization of supply chain risk ans risk management. In C. Brindley (Hrsg.), *Supply chain risk* (S. 14–27). Abingdon/Oxon: Taylor and Francis.
- Pfohl, H.-C. (2007). Supply Chain Risiko Management. In I. Hausladen & N. Abdelkafi (Hrsg.), *Produktion und Logistik* (S. 1135–1157). München: TCW Transfer-Centrum.
- Pfohl, H.-C. (2010). *Logistiksysteme: Betriebswirtschaftliche Grundlagen*. Berlin: Springer.
- Pfohl, H.-C., Gallus, P., & Köhler, H. (2007). Implementierung eines Supply Chain Risikomanagements. Theoretische Grundlagen und Ansätze zur organisatorischen Umsetzung. In T. Wimmer (Hrsg.), *Effizienz - Verantwortung - Erfolg: 24. Deutscher Logistik-Kongress Berlin [und] Eurolog; [17. - 19.10.2007]; Kongressband* (S. 191–224). Hamburg: Deutscher Verkehrsverlag.
- Pfohl, H.-C., Gallus, P., & Köhler, H. (2008a). Konzeption des Supply Chain Risikomanagements. In H.-C. Pfohl (Hrsg.), *Sicherheit und Risikomanagement in der Supply Chain: Gestaltungsansätze und praktische Umsetzung* (S. 7–94). Hamburg: DVV-Media-Group Dt. Verkehrsverlag.
- Pfohl, H.-C., Gallus, P., & Köhler, H. (2008b). Risikomanagement in der Supply Chain - Status Quo und Herausforderungen aus Industrie-, Handels- und Dienstleisterperspektive. In H.-C. Pfohl (Hrsg.), *Sicherheit und Risikomanagement in der Supply Chain: Gestaltungsansätze und praktische Umsetzung* (S. 95–147). Hamburg: DVV-Media-Group Dt. Verkehrsverlag.
- Robold, M. (2010). Transportversicherung. In M. Lange & M. Robold (Hrsg.), *Sachversicherungen für private und gewerbliche Kunden: Fach- und Führungskompetenz für die Assekuranz; geprüfter Fachwirt für Versicherungen und Finanzen, geprüfte Fachwirtin für Versicherungen und Finanzen* (S. 212–278). Karlsruhe: VVW.

- Rotter, E. (2019). *Continental gewinnt VDA Logistik Award 2019* (vom 06.02.2019). <https://www.vda.de/de/presse/Pressemeldungen/20190206-continental-gewinnt-vda-logistik-award-2019.html>. Zugegriffen am 10.05.2019.
- Sheffi, Y. (2001). Supply chain management under the threat of international terrorism. *The International Journal of Logistics Management*, 2, 1–11.
- Skorna, A. C. H. (2016). Versicherungen als mögliche risikopolitische Maßnahme: Von der Transportversicherung zu neuen Ansätzen in der Betriebsunterbrechungsversicherung. In M. Huth & F. Romeike (Hrsg.), *Risikomanagement in der Logistik: Konzepte - Instrumente - Anwendungsbispiele* (S. 209–224). Wiesbaden: Springer Gabler.
- Speckmann, R. E., & Davis, E. W. (2004). Risky business. Expanding the discussion on risk and the extended enterprise. *International Journal of Physical Distribution & Logistics Management*, 5, 414–433.
- Svensson, G. (2000). A conceptual framework for the analysis of vulnerability in supply chains. *International Journal of Physical Distribution & Logistics Management*, 9, 731–749.
- Wagner, S. M., & Bode, C. (2007). Empirische Untersuchung von SC-Risiken und SC-Risikomanagement in Deutschland. In R. Vahrenkamp & M. Amann (Hrsg.), *Risikomanagement in Supply Chains: Gefahren abwehren, Chancen nutzen, Erfolg generieren* (S. 59–79). Berlin: E. Schmidt.
- Ziegenbein, A. (2007). *Supply Chain Risiken: Identifikation, Bewertung und Steuerung*. Zürich: vdf Hochschulverlag.
- Zimmer, R. (2017). Supply Chain Risk Management - Ein Gewinn für Unternehmen und Versicherer. *Die Versicherungspraxis*, 1.
- Zsidisin, G., Ragatz, G. L., & Melnyk, S. A. (2005). The dark side of supply chain management. *Supply Chain Management Review*, 2, 46–52.

Christian Müller verantwortet seit November 2011 den Bereich Sachversicherung bei der Continental Versicherungsdienst GmbH (CVD) und ist zudem für die spartenübergreifende Betreuung der Konzerngesellschaften in Fernost und Südostasien zuständig. Nach seinem Eintritt in den Continental-Konzern im April 2008 war sein Dienstsitz vorübergehend Shanghai, wo er in den Jahren 2010 und 2011 eine koordinierende Repräsentanz des CVDs aufbaute. Begonnen hat er seine berufliche Laufbahn bei der HDI-Gerling Industrie Versicherung AG in Stuttgart, wo er im Bereich Sachversicherung tätig war. Christian Müller absolvierte ein Studium der Betriebswirtschaft in der Fachrichtung Versicherung an der Dualen Hochschule Baden-Württemberg in Stuttgart.

Jan Tschöpe hat im September 2020 sein Masterstudium im Fach Risk and Insurance am Institut für Versicherungswesen der Technischen Hochschule Köln abgeschlossen. Seit Oktober 2020 arbeitet er als Associate Consultant bei der Strategieberatung 67rockwell Consulting GmbH und ist dort in Projekten der Versicherungsbranche eingesetzt. Begonnen hat er seine berufliche Laufbahn bei der Allianz Beratungs- und Vertriebs-AG, wo er als Dualer Student im Außendienst tätig war. Das Bachelorstudium absolvierte Jan Tschöpe an der Dualen Hochschule Baden-Württemberg in Mannheim im Fach Betriebswirtschaftslehre mit der Vertiefung Versicherung.



Produktrückruf und Produkthaftung, Qualitätssicherung

26

Christian Kuhrt und Monique Neußmann

Zusammenfassung

Hersteller von Produkten sind dazu verpflichtet, ihre Produkte, auch nachdem sie auf dem Markt in Umlauf gebracht wurden, weiterhin zu beobachten. Diese Verpflichtung ist die sogenannte Produktbeobachtungspflicht. Sollte sich nach dem Inverkehrbringen des Produkts eine Fehlerhaftigkeit zeigen, ergeben sich für den Hersteller verschiedene Reaktionspflichten, wie zum Beispiel zur Produktionsumstellung oder eine Warnpflicht. Wird die Gesundheit oder die Sicherheit des Verwenders des Produkts oder eines Dritten durch das Produkt gefährdet, besteht für den Hersteller eine Verpflichtung zum Rückruf der betroffenen Produkte. Diese Verpflichtung kann durch eine behördliche Anordnung ausgelöst werden.

Um eine gesundheitsgefährdende oder sicherheitsgefährdende Fehlerhaftigkeit des Produkts frühzeitig zu erkennen, ist es wichtig, eine dauerhafte Produktbeobachtung nach dem Inverkehrbringen des Produkts auf dem Markt im Unternehmen zu integrieren, damit das Unternehmen im Falle einer Fehlerhaftigkeit schnell agieren kann. Hierzu sollte das Unternehmen die Ergebnisse in Form einer Risikoabschätzung bewerten und die notwendigen Maßnahmen zur Beseitigung des Problems ergreifen. Zu diesen Maßnahmen gehört unter anderem der Rückruf der fehlerhaften Produkte. Diese Aufgaben gehören zum Rückrufmanagement und sollen ein Unternehmen in die Lage versetzen, in Krisensituationen schnell und professionell agieren zu können. Eine wichtige Rolle spielt hierbei auch professionelles Kommunikationsmanagement.

C. Kuhrt (✉)

DMK Versicherungskontor GmbH, Bremen, Deutschland

E-Mail: christian.kuhrt@dmk.de

M. Neußmann

TH Köln, Institut für Versicherungswesen, Köln, Deutschland

Produktrückrufe können jedoch durch ein im Unternehmen integriertes Qualitätsmanagementsystem oftmals bereits im Vorfeld verhindert werden, da bei einem guten Qualitätsmanagementsystem das Produkt während des gesamten Produktionsprozesses immer wieder kontrolliert wird. Dadurch kann eine Fehlerhaftigkeit des Produkts bereits frühzeitig erkannt werden. Sollte es jedoch trotzdem zu einem Produktrückruf kommen, kann sich das Unternehmen mit speziellen Versicherungslösungen gegen das finanzielle Risiko eines Rückrufs absichern.

26.1 Einleitung

„Deutschlandweiter Rückruf von belasteter Milch“ lautet eine Schlagzeile von Zeit Online am 11.10.2019. Aufgrund eines gesundheitsschädlichen Bakterienbefalls fettarmer Frischmilch musste die DMK Group deutschlandweit die betroffenen Produkte zurückrufen (Zeit Online 2019). Aber auch andere Branchen, wie beispielsweise die Automobil- oder Spielzeugindustrie, sind immer häufiger vom Thema „Produktrückruf“ betroffen. So lautet eine Schlagzeile von Spiegel Online am 21.07.2019; „Volvo muss eine halbe Million Autos nachrüsten“. Der Automobilhersteller musste aufgrund der möglichen Gefahr von Motorbränden weltweit etwa eine halbe Million Fahrzeuge in die Werkstätten zurückrufen. Allein in Deutschland seien hiervon rund 54.000 Fahrzeuge betroffen gewesen (Spiegel Online 2019b).

Dieses Kapitel soll einen Überblick über die möglichen Haftungsgründe eines Produktherstellers, das Krisenmanagement im Falle eines Produktrückrufs, vorbeugende Maßnahmen zur Verhinderung von Produktrückrufen und eine mögliche Absicherung durch eine Versicherungslösung bieten.

26.2 Abgrenzung Produkthaftung und Produktrückruf

Die Begriffe Produkthaftung und Produktrückruf sind nicht gleichzusetzen. Der Produktrückruf ist vielmehr eine Verpflichtung, die sich aus der Produkthaftung ergeben kann. Die Produkthaftung allein zwingt den Hersteller daher nicht gleich zu einem Rückruf eines Produkts.

Um den Zusammenhang zwischen der Produkthaftung und dem Produktrückruf zu verstehen, muss daher zunächst die mögliche Haftung des Herstellers für seine Produkte betrachtet werden.

26.2.1 Unterscheidung zwischen der Produkthaftung und dem Produktrückruf

Die Produkthaftung ergibt sich zum einen aus der Haftung nach dem Produkthaftungsgesetz (ProdHaftG) und zum anderen aus der Haftung nach §§ 823 ff. BGB (Produzentenhaftung).

Im deutschen Recht ist die Produkthaftung deliktisch. Somit spielen hierbei vertragliche Ansprüche im Regelfall keine Rolle. Jedoch schließt die Delikthaftung vertragliche

Ansprüche nicht aus. Darüber hinaus bleibt das allgemeine Deliktsrecht gemäß § 15 Abs. 2 ProdHaftG von den Regelungen des Produkthaftungsgesetzes unberührt.

Das Produkthaftungsgesetz stellt eine spezielle Gefährdungshaftung dar. Der Hersteller haftet hierbei für Folgeschäden aus der Benutzung seiner Produkte. Im Gegensatz zur Haftung aus §§ 823 ff. BGB haftet der Hersteller gemäß Produkthaftungsgesetz verschuldensunabhängig und somit auch für sogenannte „Ausreißer“.

Voraussetzungen für die Haftung nach dem Produkthaftungsgesetz sind zum einen, dass es gemäß § 2 ProdHaftG ein Produkt gibt und dass dieses Produkt gemäß § 3 ProdHaftG fehlerhaft ist. Eine spätere Verbesserung des Produkts durch den Hersteller ist dagegen noch kein Indiz für eine Fehlerhaftigkeit, da für die Haftung gemäß § 3 Abs. 2 ProdHaftG stets auf den Zeitpunkt des Inverkehrbringens des Produkts abgestellt wird.

Da es sich bei der Anwendung des Produkthaftungsgesetzes um eine Gefährdungshaftung handelt, haftet der Hersteller auch für Fabrikationsfehler, die trotz aller zumutbaren Vorkehren unvermeidbar sind. Diese Fehler werden als sogenannte „Ausreißer“ bezeichnet. Werden die Voraussetzungen nach dem Produkthaftungsgesetz erfüllt, muss der Hersteller Schadenersatz leisten. Hierbei ist jedoch zu beachten, dass die Produkthaftung gemäß § 1 Abs. 1 ProdHaftG den wichtigsten Anwendungsbereich bei der Verursachung von körperlichen Schäden hat, da die Ersatzfähigkeit von Sachschäden eingeschränkt ist. Laut § 11 ProdHaftG gilt bei Sachschäden eine Selbstbeteiligung des Geschädigten. Allerdings wird auch die Schadenersatzleistung des Herstellers bei Personenschäden nach § 10 ProdHaftG begrenzt.

Durch die Begrenzungen der Schadenersatzleistungen aus dem Produkthaftungsgesetz spielt in der Praxis die deliktische Haftung, also die Produzentenhaftung nach §§ 823 ff BGB, eine weit bedeutendere Rolle.

Für einen Haftungsanspruch gemäß §§ 823 ff BGB müssen folgende Voraussetzungen erfüllt sein: Zum einen muss eine Pflichtverletzung des Herstellers und die Fehlerhaftigkeit des Produkts zum Zeitpunkt des Inverkehrbringens vorliegen. Des Weiteren muss eine Kausalität zwischen der Pflichtverletzung und dem Produktfehler vorhanden sein. Darüber hinaus muss eine Rechtsgutverletzung vorliegen. Auch hier muss eine Kausalität der Fehlerhaftigkeit vorliegen. Zudem muss ein Verschulden festgestellt sein.

Der Hersteller ist nun dazu verpflichtet, alles Erforderliche und ihm Zumutbare zu tun, um in seinem Herrschaftsbereich eine Ursache für eine Verletzung der in § 823 BGB genannten Rechte und Rechtsgüter zu verhindern. Hierbei wird zwischen unterschiedlichen Pflichten, deren Verletzung zu verschiedenen Fehlern führen kann, unterschieden:

- **Konstruktionsfehler:** Um einen Konstruktionsfehler zu vermeiden, ist der Hersteller dazu verpflichtet, dass das von ihm in Verkehr gebrachte Produkt das erforderliche Sicherheitsniveau erreicht. Hierbei hat er die Anforderungen gesetzlicher Bestimmungen und verbindlicher Normen einzuhalten und fortlaufend Überprüfungen durchzuführen.
- **Fabrikationsfehler:** Für Fabrikationsfehler haftet der Hersteller, wenn nur einzelne Produkte des Herstellers fehlerhaft sind. Hierbei geht es also um Fehler in der Produktion. Daraus leitet sich zudem eine Pflicht des Herstellers zur fortlaufenden Qualitätsüberwachung ab.

- **Instruktionsfehler:** Bei einer mangelhaften Gebrauchsanweisung liegt ein Instruktionsfehler vor. Der Hersteller hat die Pflicht, den Verbraucher über die sicherheitsrelevanten Eigenschaften des Produkts zu informieren, damit dieser zu einem sachgerechten Umgang in der Lage ist. Diese Informationspflicht schließt auch die Warnpflicht über einen vorhersehbaren Fehlgebrauch des Produkts mit ein.
- **Entwicklungsfehler:** Der Hersteller haftet nicht für die sogenannten Entwicklungsfehler. Das bedeutet, dass er nicht für Fehler haftet, die erst aufgrund weiteren technischen Fortschritts erkennbar werden. Dabei muss sichergestellt sein, dass diese zum Zeitpunkt des Inverkehrbringens des Produkts noch nicht erkennbar waren.

Aus den genannten möglichen Produktfehlern ergibt sich eine **Produktbeobachtungspflicht des Herstellers**. Der Hersteller ist zur Beobachtung der weiteren Entwicklung des Produkts verpflichtet. Er muss somit das Verhalten des Produktes am Markt beobachten, damit er frühzeitig eventuelle Konstruktions-, Fabrikations- oder Instruktionsfehler erkennen kann. Aus dieser Verpflichtung können sich Reaktionspflichten ergeben. Eine Reaktionspflicht kann sich in Form einer Produktionsumstellung, einer Warnpflicht oder sogar einer Rückrufpflicht äußern, wenn nur so schwere Schäden für den Benutzer oder Dritte abgewehrt werden können (vgl. Poller 2016, Rn. 99–125).

Die Pflicht des Herstellers zu einem Produktrückruf ergibt sich somit aus der Produktbeobachtungspflicht und der damit verbundenen Reaktionsverpflichtung. Es stellt sich nun die Frage, wann genau der Hersteller zu einem Produktrückruf verpflichtet ist.

26.2.2 Verpflichtung zum Produktrückruf

Wie bereits im vorherigen Abschnitt beschrieben, leitet sich die Rückrufpflicht des Herstellers aus der privatrechtlichen Verpflichtung zum Rückruf gefährlicher Produkte aus der deliktsrechtlichen Verkehrssicherungspflicht im Rahmen des § 823 Abs. 1 BGB ab. Diese Verpflichtung resultiert aus der sogenannten Produktbeobachtungspflicht.

Darüber hinaus kann sich eine Rückrufpflicht auch aus einer behördlichen Anordnung gemäß § 26 Abs. 2 Nr. 7 ProdSG ergeben. Die Auslösung einer Rückrufaktion durch eine öffentlich-rechtliche Anordnung der Behörde nach dem ProdSG ergibt sich daraus, dass laut § 3 Abs. 1 ProdSG Produkte nur dann auf dem Markt bereitgestellt werden dürfen, wenn bei bestimmungsgemäßer Verwendung oder vorhersehbarer Fehlanwendung des Produkts die Sicherheit und Gesundheit der Verwender oder Dritter nicht gefährdet wird. Sollte ein Produkt nicht diesen Anforderungen entsprechen, muss die zuständige Behörde gemäß § 26 Abs. 4 ProdSG neben anderen Maßnahmen auch den Rückruf des in Verkehr gebrachten Produkts anordnen (vgl. Röbe-Oltmanns und Schimikowski 2017, S. 115 ff.).

Neben dem Hersteller kann auch der Händler von einer Rückrufpflicht betroffen sein. Laut § 27 ProdSG kann die Behörde ihre Rückrufanforderungen auch an den Händler richten, falls eine Gefahr nicht durch den Zugriff auf den verantwortlichen Hersteller des Produkts beseitigt werden kann.

Rückrufaktionen werden in der Praxis auch regelmäßig von den Herstellern des Endprodukts durchgeführt, das heißt von den Herstellern am Ende einer Produktionskette. In diesem Fall kann ein fehlerhaftes Zulieferteil, das für die Herstellung des Endprodukts verwendet wurde, für den Produktfehler ursächlich sein. Die Kosten einer Rückrufaktion können hierbei im Regressweg gegen den Zulieferer geltend gemacht werden. Dieser Regressanspruch ergibt sich aus §§ 840 und 426 BGB.

Grundsätzlich wird zwischen zwei Arten eines Rückrufs unterschieden. Zum einen gibt es den stillen Rückruf. Hierbei erfolgt der Rückruf durch den Hersteller, Händler oder Importeur durch eine gezielte Ansprache der Zwischenhändler oder sonstigen Serviceverantwortlichen. Der eigentliche Produktabnehmer erfährt dabei nichts von dem Rückruf. Zum Teil wird bei fälligen Revisionsarbeiten dann der Sachmangel behoben, sofern diese zeitliche Verzögerung ohne Sicherheitsbedenken hingenommen werden kann.

Neben dem stillen Rückruf gibt es noch den offenen Rückruf, auch als öffentlicher Rückruf bezeichnet. Hierbei erfolgt der Rückruf durch den Hersteller, Händler oder Importeur mittels öffentlich zugänglicher Medien (vgl. Röbe-Oltmanns und Schimikowski 2017, S. 119 ff.). Bei einem offenen Rückruf wird somit der Produktabnehmer direkt angesprochen.

Naturgemäß haben Hersteller ein Interesse, die Art des Produktrückrufs zu beeinflussen, da jeder Rückruf zugleich eine Gefahr für einen Image- und Reputationsschaden bedeutet. Ein Hersteller von Milchprodukten wird beispielsweise bei einem Verdacht des Inverkehrbringens fehlerhafter aber ungefährlicher Produkte zunächst zwingend den zuständigen Veterinär kontaktieren. Die offene und vertrauensvolle Zusammenarbeit zwischen dem Hersteller und dem Veterinär ist eine wesentliche Grundvoraussetzung für eine konstruktive Beratung im jeweiligen Einzelfall. Kann der Hersteller dem Veterinär plausibel darlegen, dass die Produkte noch nicht beim Endverbraucher angekommen sind, sondern sich beispielsweise noch im Zentrallager oder in der Auslieferung befinden, kann er um einen stillen Rückruf bitten. Der Veterinär kann diesem zustimmen. Der Verbraucherschutz bleibt natürlich auch hierbei das oberste Ziel.

Anders sieht es bei gesundheitsgefährdenden Produkten aus. Wird beispielsweise ein unabhängiges Prüflabor von dem Hersteller mit der Prüfung von Lebensmitteln beauftragt und stellt sich bei dieser Prüfung eine wirkliche Gesundheitsgefährdung des Verbrauchers dar, ist das Prüflabor sofort dazu verpflichtet, den Hersteller und den Veterinär zu kontaktieren. Ein stiller Rückruf ist hierbei ausgeschlossen.

26.3 Praxisbeispiele zum Produktrückruf

Immer wieder tauchen in den Medien Warnungen auf, wie zum Beispiel „Tückische Gefahr: ALDI NORD informiert zu möglichen Glassplittern in SÖLDE Hähnchenschnitzeln“ (Produktrückrufe 2019a) oder „Erneut Verdacht auf Kolibakterien (VTEC) in IGLO Petersilie (TK): Vor dem Verzehr wird gewarnt!“ (Produktrückrufe 2019b).

Verbraucher können sich in Deutschland täglich über das Portal **Produktrueckrufe.de** zu Produktwarnungen, Sicherheitshinweisen und Rückrufaktionen informieren und sich dadurch frühzeitig vor Gefährdungen durch die genannten Produkte schützen (vgl. Heide-mann 2018). Produktrückrufe sind somit für den Verbraucher aufgrund der medialen Wirkung eines öffentlichen Rückrufs allgegenwärtig.

Im Jahr 2016 wurden allein 148 Lebensmittel in Deutschland öffentlich zurückgerufen. Das war laut dem Bundesamt für Verbraucherschutz und Lebensmittelsicherheit (BVL) im Vergleich zum Jahr 2015 eine Steigerung um fast 50 Prozent (vgl. Dogan 2017).

Ein Grund für den Anstieg von Produktrückrufen besteht möglicherweise in der immer stärker werdenden Komplexität der Produkte. Immer mehr Produkte bestehen aus fragilen Werkstoffen oder setzen sich aus Nano-Bestandteilen zusammen. Zudem bestehen viele Produkte aus elektrischen, elektronischen und/oder informationstechnologischen Bestandteilen. All diese Bestandteile weisen unter Umständen sicherheitskritische Fehler auf. Ein weiterer Aspekt ist, dass oftmals die Bestandteile eines Produkts nicht vom Endprodukt hersteller selbst, sondern von Lieferanten oder den Zulieferern des Lieferanten hergestellt und anschließend im Produkt des Endherstellers verbaut werden. Eventuelle Sicherheitsprobleme dieser Bestandteile werden somit erst beim Gebrauch/ oder Verbrauch des Endprodukts identifiziert. Ein weiterer Grund für den Produktrückrufanstieg ist das gestiegene Verbraucherinteresse. Mit vermehrter Selbstverständlichkeit nehmen Verbraucher an, dass die Verantwortung für ein fehlerhaftes Produkt vom Produzenten übernommen wird. Dabei wird die eigentliche Schuldfrage des Herstellers außer Acht gelassen. Hersteller müssen sich daher stärker dem Risikopotenzial eines Produkts widmen (vgl. Glasl und Klindt 2012, S. 10 f.).

Während des Produktionsprozesses kann es gerade in der Lebensmittelindustrie schnell zu einer (durch Mitarbeiter) versehentlichen oder vorsätzlichen Kontamination der Lebensmittel kommen (vgl. Dogan 2017). Gerade kontaminierte oder verdorbene Lebensmittel stellen ein erhebliches Gesundheitsrisiko für den Verbraucher dar und müssen daher zwingend vom Händler oder Hersteller zurückgerufen werden.

So ruft der Hersteller Lincet seit dem 10.05.2019 seinen Chaource Käse der Handelsmarken Tradition Emotion, Cremier und Tradition aufgrund einer möglichen Kontamination mit E.Coli Bakterien zurück. Durch den Verzehr von Lebensmitteln, die durch E.Coli Bakterien kontaminiert wurden, können dramatisch verlaufenden Durchfallerkrankungen beim Kunden hervorgerufen werden (Produktwarnungen 2019c). Gerade für Kinder unter sechs Jahren und ältere Menschen kann sich dies zu einer lebensbedrohlichen Erkrankung entwickeln. Seit dem 3. Mai 2019 ruft die Francia Mozzarella GmbH mit Sitz in Berlin den hergestellten Schafskäse mit schwarzem Pfeffer aufgrund einer Kontamination mit E.Coli Bakterien zurück. Diese Warnungen sind über das Informationsportal **Produkt-warnung.eu** zu finden. Ähnlich wie auf dem Rückrufportal Produktrueckrufe.de werden hier aktuelle Produktrückrufe und Verbraucherwarnungen aufgeführt.

Aber auch in anderen Branchen können fehlerhafte Produkte enorme gesundheitliche Schäden verursachen und müssen dadurch von den Herstellern zurückgerufen werden.

In der Automobilindustrie arbeiten die Fahrzeughersteller mit vielen unterschiedlichen Zulieferern beim Bau eines Fahrzeugs zusammen. Bereits ein fehlerhaftes Produkt, das durch einen Zulieferer hergestellt und im Fahrzeug verbaut wurde, kann zu einer großen Rückrufaktion des Herstellers führen.

So musste der Automobilhersteller BMW im Februar 2019 weltweit rund 480.000 Fahrzeuge aufgrund von möglicherweise gefährlichen Airbags in die Werkstätten zurückrufen. Hiervon waren allein ca. 95.000 Fahrzeuge in Deutschland betroffen. Betroffen waren die Fahrzeugreihen 5er BMW und X5 der Baujahre 2000 bis 2004 mit nicht serienmäßigen Lenkrädern. In diesen Lenkrädern wurden Airbags des inzwischen insolventen japanischen Zulieferers Takata verbaut. Diese können bei der Auslösung möglicherweise die Fahrzeuginsassen durch Metallteile schwer verletzen. Aufgrund der drohenden Personenschäden rief der Automobilhersteller die Fahrzeuge zurück, um die Lenkräder zu überprüfen. Von dieser Problematik ist allerdings nicht nur allein der Hersteller BMW betroffen, da auch andere Hersteller die Airbags des japanischen Zulieferers verbaut haben. Mehr als 42 Millionen Fahrzeuge mussten allein in den USA in den letzten Jahren aus diesem Grund zurückgerufen werden (vgl. Spiegel Online 2019a).

Auch in der Spielzeugindustrie sind Rückrufaktionen der Hersteller oder Produktanbieter für den Verbraucher allgegenwärtig. Gerade Kleinkinder sind besonderen Risiken durch ihr unbedarftes Spielverhalten ausgesetzt, da sie viele Gegenstände und so auch ihr Spielzeug in den Mund nehmen. Aus diesem Grund besteht die Gefahr, dass sie Kleinteile der Spielzeuge verschlucken. Dadurch besteht eine erhöhte Erstickungsgefahr,

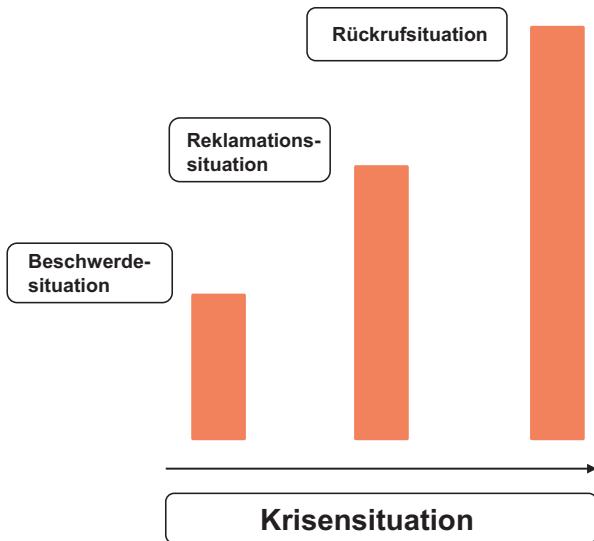
Aufgrund dieser Erstickungsgefahr für Kleinkinder musste im April 2019 der Hersteller Swissgames verschiedene Seek'o Blocks Konstruktionsspiele zu rufen. Kinder konnten mit halbkugelförmigen Stücken eine kleine Kugel herstellen. Hierbei bestand die Gefahr, dass Kleinkinder diese in den Mund nehmen und eventuell verschlucken könnten (Produktwarnungen 2019b). Auch das Unternehmen Flying Tiger Copenhagen musste im März 2019 den Artikel „Holzlok und -wagons“, der seit November 2018 verkauft wurde, aufgrund von einer Erstickungsgefahr für Kleinkinder zurückrufen (Produktwarnungen 2019a). Auch diese Rückrufaktionen sind auf dem Informationsportal **Produktwarnungen.eu** zu finden.

Von Produktrückrufen können Unternehmen in jeder Branche betroffen sein. Doch wie genau kann ein Unternehmen mit einem Rückruf umgehen? Welche Maßnahmen muss ein Unternehmen ergreifen, um die Folgen eines Produktrückrufs zu mindern? Was macht ein gut funktionierendes Rückrufmanagement aus? Wie kann ein Rückruf im Vorfeld verhindert werden? Gibt es geeignete Versicherungslösungen? Mit der Klärung genau dieser Fragen beschäftigen sich die nun folgenden Abschnitte.

26.4 Krisenfall „Produktrückruf“

Gerade die Medienberichterstattung in Bezug auf das zurückgerufene Produkt kann langfristig oftmals schwerwiegende und unvorhersehbare Folgen für ein Unternehmen haben. Neben den hohen Kosten für den Produktrückruf ist das Unternehmen auch zahlreichen

Abb. 26.1 Entwicklung von Produktkrisen. (Quelle: eigene Darstellung in Anlehnung an Glasl und Klindt 2012, S. 28)



weiteren Risiken ausgesetzt. Vor allem die wirtschaftlichen Folgen durch einen Image- oder Markenschaden werden erst nach dem Rückruf erkennbar (vgl. Dogan 2017).

Wird der Begriff „Krise als eine unsichere Situation definiert, deren weiterer Verlauf von Entscheidungen in einem unklaren Umfeld abhängt, ist anhand Abb. 26.1 zu erkennen, dass eine Krisensituation im Unternehmen schon bei einer Beschwerdesituation vorliegt“. Diese Beschwerdesituation drückt sich in einem Unbehagen oder Missfallen des Verbrauchers mit dem Produkt aus. Hierbei fehlt es jedoch an einem Produktmangel oder Schaden. Die nächste Stufe einer Krisensituation stellt die Reklamationssituation dar. Im Falle einer Reklamation existiert bereits ein tatsächlicher Mangel am Produkt oder ein Schaden. Die höchste Eskalationsstufe einer Produktkrisensituation stellt jedoch die Rückrufsituation dar, da hier das Produkt einen sicherheitsrelevanten Fehler aufweist, der zu Personenschäden führen kann (vgl. Glasl und Klindt 2012, S. 25 ff.).

Vor allem in den zunehmenden Krisensituationen ist ein schnelles Eingreifen des Krisenmanagements im Unternehmen notwendig. Gerade im Fall eines Produktrückrufs ist dieses schnelle Eingreifen von großer Bedeutung.

Wie das Krisenmanagement hinsichtlich eines Produktrückrufs im Unternehmen umgesetzt werden kann, wird in den folgenden Abschnitten dargestellt.

26.4.1 Rückrufmanagement im Unternehmen

In § 6 Abs. 2 ProdSG wird die gesetzliche Forderung nach einem Rückrufmanagement geregelt. Demnach haben „der Hersteller, sein Bevollmächtigter und der Einführer (... jeweils im Rahmen ihrer Geschäftstätigkeit Vorkehrungen für geeignete Maßnahmen zur Vermeidung von Risiken zu treffen, die mit dem Verbraucherprodukt verbunden sein können, das sie auf dem Markt bereitgestellt haben; die Maßnahmen müssen den Produktei-

genschaften angemessen sein und reichen bis zur Rücknahme, zu angemessenen und wirksamen Warnungen und zum Rückruf. Das ProdSG beschränkt diese Forderung zwar auf Verbraucherprodukte, jedoch sollte die Sicherheit des Produkts bzw. der Schutz vor Gefahren durch einen unsicheren Produktzustand nach dem Inverkehrbringen des Produkts am Markt vor dem Hintergrund der Produzentenhaftung für alle Produkte gewahrt werden (vgl. Klindt und Wende 2014, S. 49)“.

Der Begriff „Rückrufmanagement“ bezeichnet ein System von Abläufen bzw. Prozessen in einem Unternehmen. Mit diesem System soll das Unternehmen in die Lage versetzt werden, in einem Krisenfall angemessen agieren zu können. Hierbei soll das Unternehmen so organisiert werden, dass es in der Lage ist:

- bei drohenden Personen- oder Sachschäden die Sicherheit der im Verkehr befindlichen Produkte durch unverzügliche Maßnahmen wiederherzustellen;
- die erforderlichen Ressourcen zur Durchführung der Maßnahmen im Unternehmen zu haben;
- die Verwender des Produkts vollständig über die drohende Gefahr und Durchführung der Maßnahmen zu informieren;
- die gesetzlichen Vorschriften zur Produktsicherheit zu befolgen und die Verpflichtungen zur behördlichen Meldung von Produktgefahren einzuhalten.

Das Rückrufmanagement ist somit der Oberbegriff für eine im Unternehmen zu implementierende Organisationsstruktur. Diese ist der Schlüssel zum Erfolg, damit ein Unternehmen einen Krisenfall angemessen meistern kann (vgl. Klindt und Wende 2014, S. 104 f.).

Es lassen sich hierbei drei konkrete Aufgabenbereiche für das Rückrufmanagement ableiten:

1. **Produktbeobachtung:** Das Unternehmen soll das Verhalten des Produkts im Markt beobachten und dadurch frühzeitig sicherheitsrelevante Auffälligkeiten erkennen.
2. **Risikoabschätzung:** Hierbei sollen die Beobachtungsergebnisse der Produktbeobachtung systematisch bewertet werden, um über die Notwendigkeit weiterführender Maßnahmen zu entscheiden.
3. **Weiterführende Maßnahmen:** Das Unternehmen entscheidet, ob ein normales Änderungsprozedere stattfindet oder eine Warnung, Rücknahme oder ein Rückruf des Produkts durchgeführt wird. Zu beachten ist dabei die Meldepflicht des Herstellers bei Verbraucherprodukten (vgl. Klindt und Wende 2014, S. 49 f.).

Doch welche konkreten Maßnahmen muss ein Unternehmen nun in dem jeweiligen Aufgabenbereich treffen?

Die **Produktbeobachtung** stellt eine Informationserfassung mit der Zielsetzung dar, die Sicherheit des Anwenders von durch den Hersteller in Verkehr gebrachten Produkten zu wahren. Aus diesem Grund konzentriert sich die Informationserfassung auf Beobachtungen, die ein sicherheitsrelevantes Potenzial besitzen. Das Unternehmen muss diesbzgl. zunächst

für das Produkt bzw. für das Produktpotfolio einen Katalog mit sicherheitsrelevanten Aspekten erstellen und den mit der Produktbeobachtung betrauten Stellen im Unternehmen zur Verfügung stellen. In diesem Katalog stellt das Unternehmen einen möglichen Schaden und die daraus resultierende Gefährdung für den Verbraucher gegenüber. So kann ein Schaden an elektrischen Isolationen oder Strom führenden Produkten zu einer Gefährdung des Verbrauchers in Form eines Stromschlags, einer Funkenbildung und Brandgefahr führen.

Im Anschluss der Erstellung eines Katalogs sicherheitsrelevanter Schäden für die Produkte schließt sich die Installation einer Produktbeobachtung an. Diese umfasst die Aufgaben, die Informationen gemäß dem Schadenkatalog im Markt zu erfassen, diese im Unternehmen an eine zentrale Stelle zu übermitteln und anschließend die Informationen angemessen im Unternehmen zu verarbeiten. Neben der Auswertung von Produktbeschwerden aus dem Markt umfasst die Produktbeobachtung auch die Durchführung von Stichproben.

Die Produktbeobachtungspflicht des Unternehmens beginnt mit dem Inverkehrbringen des Produkts im Markt und umfasst die erwartete Lebensdauer des Produkts. Hierbei ist zu beachten, dass bei langlebigen Produkten die Verjährungsfristen aus dem Deliktsrecht zu beachten sind (vgl. Klindt und Wende 2014, S. 53 f.).

Abb. 26.2 zeigt den Umgang eines Herstellers mit Informationen über potenzielle sicherheitsrelevante Produktauffälligkeiten im Zuge der Produktbeobachtung. Die Kernauf-

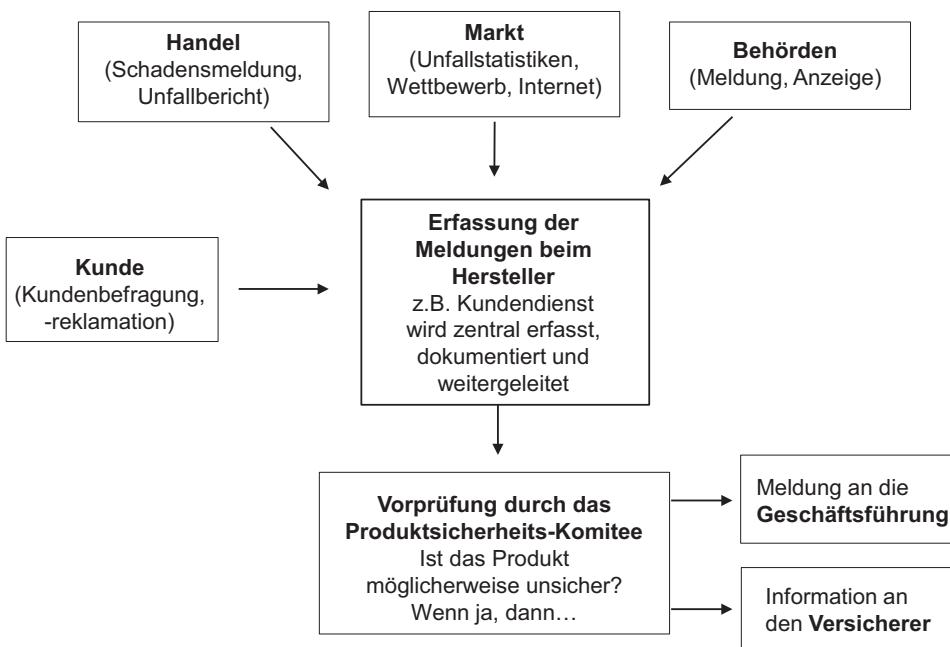


Abb. 26.2 Ablaufplan Produktbeobachtung. (Quelle: eigene Darstellung in Anlehnung an Klindt und Wende 2014, S. 60)

gabe im Umgang mit diesen Informationen besteht vor allem darin, die produktintegritätsrelevanten Fakten prozesssicher herauszufiltern und an eine zentrale Stelle zur weiteren Bearbeitung zu übermitteln. Dabei muss der Hersteller darauf achten, dass keine kritischen Meldungen vom Markt verloren gehen (vgl. Klindt und Wende 2014, S. 59).

Im Rahmen der Produktbeobachtung ist auf eine frühzeitige Weiterleitung von Informationen über mögliche Krisensituationen an die Geschäftsleitung des Unternehmens zu achten. Eine rechtzeitige Einbeziehung der Unternehmensleitung gibt dieser die Möglichkeit, direkt zu Beginn einer sich entwickelnden Krise involviert zu sein und den Vorgang mit einer notwendigen Priorität zu verfolgen.

Das Unternehmen muss während der Produktbeobachtung jede erhaltene Schadensmeldung umgehend hinsichtlich einer vermuteten Unsicherheit bzw. eines Fehlers des Produkts prüfen. Sollte ein Personen- oder Sachschaden gemeldet werden, ist es ratsam, den Versicherer bereits frühzeitig zu informieren. Falls kein fehlerhafter Zustand bei dem gemeldeten Produkt vorliegt, kann die Schadensmeldung in den normalen Reklamationsabwicklungsprozess überführt werden (vgl. Klindt und Wende 2014, S. 60 f.).

Für die Auswertung der Produktbeobachtung ist es wichtig, dass der Hersteller die Produkte auf ein bestimmtes Herstell-Los (Charge) zurückverfolgen kann. Diese Rückverfolgbarkeit der Produkte ist ein wichtiges Instrument, um ein effizientes und professionelles Rückrufmanagement sicherstellen zu können. Ist ein Hersteller nicht dazu in der Lage, seine Produkte zuverlässig zu identifizieren und einem genauen Fertigungsumfang zuzuordnen, handelt er bei einer Schadensmeldung und einer damit verbundenen möglichen Fehlerhaftigkeit seines Produkts blind.

Sollte es nun zu einem Produktrückruf kommen, muss der Hersteller einen unverhältnismäßigen Aufwand betreiben, da die betroffene Produktcharge nicht gezielt angesprochen werden kann und dadurch der betroffene Warenumfang deutlich erweitert werden muss (vgl. Klindt und Wende 2014, S. 62). Dies wäre zum Beispiel der Fall, wenn ein Lebensmittelhersteller sein Produkt aufgrund einer drohenden Gesundheitsgefährdung der Verbraucher, zum Beispiel durch E.Coli Bakterien kontaminierte Lebensmittel, zurückrufen muss und nicht genau feststellen kann, an welchem Tag das betroffene Produkt hergestellt wurde. Der Hersteller müsste somit im schlimmsten Fall alle Produkte, die sich im Markt befinden, zurückrufen, obwohl nur Produkte eines bestimmten Produktionstages betroffen sind.

Die Notwendigkeit der Produktrückverfolgbarkeit nimmt auch durch die fortgeschrittenen Harmonisierung des europäischen Produktsicherheitsrechts zu, da durch die Rückverfolgbarkeit das Aufspüren der Produktverantwortlichen durch die Marktüberwachungsbehörden erleichtert wird. Für ein Unternehmen ist es daher von Bedeutung, jederzeit ermitteln zu können, wie viele und welche Produkte in den Ländern vertrieben wurden, um auf Informationsanfragen der Marktüberwachungsbehörden reagieren zu können.

Aus diesem Grund wird ein Produkt mittels Kennzeichnung einer bestimmten Charge zugeordnet. Diese Kennzeichnung umfasst folgende Daten:

- Herstelldatum (Herstellungslos),
- Fertigungsdaten (Stückliste),
- Material (Chargendaten).

Die Kennzeichnung ermöglicht es dem Unternehmen, ein am Markt beobachtetes Produkt, das möglicherweise schadhaft ist, einem bestimmten Herstellungslos zuzuordnen. Der Hersteller kann dadurch das mögliche Schadenausmaß der betroffenen Produkte ermitteln und bei einem eventuellen Produktrückruf genau die betroffenen Produkte identifizieren.

Mittels der Produktbeobachtung kann ein Unternehmen somit aktiv das Verhalten des Produkts am Markt verfolgen. Dadurch wird ein frühestmöglicher Einfluss des Unternehmens bei einer möglichen Fehlerhaftigkeit des Produkts möglich. Eine professionelle Produktbeobachtung ist somit eine Grundvoraussetzung für ein gut funktionierendes Rückrufmanagement (vgl. Klindt und Wende 2014, S. 62 ff.).

Der zweite Aufgabenbereich innerhalb des Rückrufmanagements ist die **Risikoabschätzung/-bewertung**. Ziel der Risikoabschätzung bzw. -bewertung ist es, das Schadenpotenzial eines unsicheren Produkts unter Berücksichtigung der Schadeneintrittswahrscheinlichkeit zu ermitteln. Das Ergebnis dieser Bewertung dient als Entscheidungsgrundlage für das weitere Vorgehen in einem Schadenfall. Gerade bei eventuell unsicheren Produkten, die bereits in Verkehr gebracht wurden, hängt jede Entscheidung des Unternehmens über mögliche Maßnahmen, wie zum Beispiel dem Produktrückruf, von diesem Ergebnis ab.

Durch die objektive Risikoabschätzung werden sowohl panische Überreaktionen bei hypothetisch möglichen Gefährdungen durch das Produkt, als auch leichtfertige Verharmlosungen bei schwerwiegenden Risiken vermieden.

Diese Risikoabschätzung sollte durch ein Team von Mitarbeitern erfolgen, die folgende Voraussetzungen erfüllen:

- Produktkenntnisse,
- Erfahrung im Umgang mit Risikoeinschätzungen,
- Verständnis dafür, dass mögliche Entscheidungen hinsichtlich einer falschen Risikobeurteilung eines Produkts rechtliche Konsequenzen haben können.

Bei Bedarf kann dieses kleine, fest installierte Team um Fachleute, die sich mit dem jeweiligen konkreten Problem auskennen, ergänzt werden (vgl. Klindt und Wende 2014, S. 64 ff.).

Das Unternehmen kann die Risikobewertung mithilfe von unterschiedlichen Vorgehensweisen durchführen. Hierzu zählt zum einen eine Risikoanalyse, die auf einem zweistufigen Ansatz basiert, der die beiden Parameter Schadensumfang und Auftretenswahrscheinlichkeit des Schadensumfangs zur Beurteilung des Risikos verknüpft. Der Schadensumfang steht hierbei für das Gefährdungspotenzial eines Schadens resultierend aus dem unsicheren Produktzustand (vgl. Klindt und Wende 2014, S. 66). Zum anderen zählt hierzu eine Risikobewertung nach dem RAPEX-Leitfaden der Europäischen Kommission. Diese beruht auf einer

Vorgabe der Europäischen Kommission, die Ende 2009 verabschiedet wurde. Für europäische Marktüberwachungsbehörden ist der RAPEX-Leitfaden eine verbindliche Vorgabe für die Ermittlung von Produktrisiken und deren Einspeisung in die verschiedenen europäischen Meldesysteme. Diese Vorgabe ist allerdings für Hersteller, Händler und Importeure unverbindlich. Jedoch ist es empfehlenswert, den Leitfaden bei der Entscheidungsfindung zu Grunde zu legen, damit das Unternehmen der Marktüberwachungsbehörde eine Aufarbeitung des Produktrisikos ermöglichen kann. Gemäß RAPEX-Leitfadens entwickelt das Unternehmen zunächst ein oder mehrere Verletzungsszenarien. Anschließend wird diese unter Berücksichtigung der Eintrittswahrscheinlichkeit einem entsprechenden Risikograd zugeordnet. Der Risikograd, also das Gesamtrisiko, wird somit anhand des Gefährdungspotenzials des Produkts in Form einer Verletzung durch das Produkt und dessen Eintrittswahrscheinlichkeit ermittelt (vgl. Klindt und Wende 2014, S. 72).

Die Risikoeinschätzung stellt daher eine Schlüsselfunktion für den Umgang mit Problemmeldungen von Produkten in einem Unternehmen dar. Aufgrund einer Problemmeldung muss ein Unternehmen mögliche Personen- und/oder Sachschäden abwägen. Das Unternehmen muss hierfür das Gefährdungspotenzial und dessen Wahrscheinlichkeit ermitteln und hieraus die Risikohöhe ermitteln. Diese Risikohöhe entscheidet anschließend über das weitere Vorgehen des Unternehmens hinsichtlich des problembehafteten Produkts.

Das Unternehmen sollte allerdings neben der methodischen Risikobewertung auch juristische Aspekte berücksichtigen und hierzu auch die dementsprechende Kompetenz, wie zum Beispiel durch die Rechtsabteilung des Unternehmens, zu Rate ziehen (vgl. Klindt und Wende 2014, S. 80).

Den dritten und somit letzten Aufgabenbereich des Rückrufmanagements stellen die **weiterführenden Maßnahmen** dar:

Ergibt sich anhand der Risikobeurteilung, die zuvor beschrieben wurde, ein nicht vertretbares Risiko, besteht die Möglichkeit einer Gefährdung der Sicherheit der Verbraucher, unbeteiliger Dritter oder anderer Rechtsgüter. Dies stellt die Bedingung für eine entsprechende Maßnahme im Markt dar. Die Unternehmensleitung muss daher schnellstmöglich über das weitere Vorgehen entscheiden. Das Unternehmen kann hierbei unterschiedliche Maßnahmen ergreifen. Hierzu zählen zum Beispiel:

- eine Warnung des Handels bzw. der Endkunden, um auf die möglichen Gefahren hinzuweisen;
- die Rücknahme der gefährdeten Produkte, bevor sie in den Markt gerät. Der Kunde kommt somit nicht mit dem Produkt in Berührung;
- der Produktrückruf mit der Zielsetzung das Produkt zu bessern (durch eine Reparatur), auszutauschen gegen ein neues Produkt oder den Kaufpreis zu erstatten;
- bei Verbraucherprodukten besteht zudem eine Meldepflicht bei den Behörden.

Ob ein Unternehmen das Produkt zurückruft oder es zurücknimmt, hängt maßgeblich vom Aufenthaltsort des Produkts ab. Eine Rücknahme wird eingeleitet, sofern sich das Produkt noch nicht beim Verwender befinden. Dagegen ist ein Rückruf unumgänglich,

sobald vermutet werden muss, dass sich die betroffenen Produkte bereits überwiegend beim Verwender befinden (vgl. Klindt und Wende 2014, S. 80 f.).

Abschließend ist somit festzuhalten, dass das Rückrufmanagement eine gut funktionierende Organisation im Unternehmen erfordert, um ein schnelles Agieren im Schadenfall durch das Unternehmen zu ermöglichen. Das Rückrufmanagement erfordert zudem ein gutes Kommunikationsmanagement des Unternehmens. Dieses muss sowohl im Unternehmen als auch im Umgang mit der Öffentlichkeit umgesetzt werden.

Im folgenden Abschnitt wird dargestellt, wie das Kommunikationsmanagement bei einem Produktrückruf bestenfalls in einem Unternehmen integriert sein und funktionieren kann.

26.4.2 Kommunikationsmanagement im Krisenfall

Einen Teil des gesamten Krisenmanagementprozesses stellt die Krisenkommunikation dar. Im vorherigen Abschnitt wurde dargestellt, dass nicht hinnehmbare Sicherheits- und Gesundheitsrisiken eines bereits in Verkehr gebrachten Produkts zu einer weiterführenden Maßnahme im Markt, wie zum Beispiel dem Rückruf eines Produkts, führen muss. Aus der weiterführenden Maßnahme leitet sich ein entsprechendes spezifisches Kommunikationsprogramm ab.

Die Aufgabe der Krisenkommunikation ist es, eine geeignete Strategie zu entwickeln, um über mögliche Gefahren des Produkts zu informieren und das Vertrauen für die entwickelten Lösungsmodelle des Unternehmens zu gewinnen. Diese Strategie soll die Öffentlichkeit, die Medien und alle weiteren relevanten internen und externen Zielgruppen ansprechen. Zur Umsetzung dieser Strategie wird ein Maßnahmenkatalog entwickelt, in welcher Form mit den entsprechenden Zielgruppen kommuniziert werden soll. Dieser Maßnahmenkatalog umfasst zum Beispiel Kommunikationsmittel wie die Rückrufanzeige, den entsprechenden Pressetext oder auch das Mailing an den Kunden oder den Handel. Mittels einer derartigen Krisenkommunikation sollen negative Auswirkungen auf das Unternehmen, die Unternehmensmarke oder das Produkt verhindert werden. Damit gehört die Krisenkommunikation zu den wichtigsten strategischen Aufgaben.

Bei Produktrückrufen wird in der Krisenkommunikation zwischen strategischen und operativen Zielen unterschieden. Zu den strategischen internen und externen Zielen gehören folgende Aspekte:

- **das Vertrauen stärken:** Das Vertrauen soll unter anderem in das Unternehmen, die Marke, das Produkt, das Führungsmanagement und die ökonomische Zukunft des Unternehmens gestärkt werden.
- **die Glaubwürdigkeit sicherstellen:** Die Glaubwürdigkeit bei den jeweiligen Zielgruppen (zum Beispiel Kunden, Behörden, Mitarbeiter, Stakeholder, Medien) bzgl. der Korrektheit und Vollständigkeit der Argumentation zum Produktproblem und für die

Übernahme der Verantwortung und Lösungskonzepte des Unternehmens soll sichergestellt werden.

- **die Offenheit des Unternehmens gewährleisten:** Hierbei soll vor allem die Dialogbereitschaft des Unternehmens gegenüber kritischen Anfragen sichergestellt werden. Zudem soll grundsätzlich Offenheit gegenüber den Zielgruppen gewährleistet werden.

Zu den operativen internen und externen Zielen zählen zum Beispiel folgende Aspekte:

- Verhinderung negativer Schlagzeilen,
- Verhinderung von Umsatzeinbrüchen (zum Beispiel durch negative Berichterstattung),
- Abwenden negativer Effekte für die gesamten Marketingaktivitäten des Unternehmens,
- ggf. Motivation von Mitarbeitern zur engagierten Mitarbeit an der Problemlösung,
- Verhinderung weiterer Kollateralschäden für das Unternehmen. Hierzu zählen zum Beispiel die Verhinderung einer Kündigungswelle oder die Auslistungen bei Kunden (vgl. Glasl und Klindt 2012, S. 42 ff.).

Grundsätzlich stellt eine Krise im Unternehmen eine mögliche Vertrauenskrise dar. Kunden können schnell das Vertrauen in das Produkt und damit auch in das Unternehmen verlieren. Erst im Anschluss einer Krise zeigt sich, ob das Unternehmen zum Beispiel erfolgreich mit einem Produktrückruf umgegangen ist, sodass der Kunde dem Produkt und dem Unternehmen weiterhin Vertrauen schenkt. Das Kommunikationsmanagement des Unternehmens trägt hierzu maßgeblich bei. Eine gut funktionierende Meldekette innerhalb des Unternehmens ist hierbei die Grundlage für das weitere Handeln des Unternehmens. Meldungen über Produktprobleme können über verschiedene Kanäle dem Unternehmen, dem Hersteller oder einem Handelsunternehmen gemeldet werden. So können die Meldungen zum Beispiel über den Kundenservice, die Filiale, Medien oder Behörden das Unternehmen erreichen. Aus diesem Grund ist es wichtig, im Unternehmen eine sogenannte „**First-Responder-Funktion**“ zu integrieren. Diese sollte an 365 Tagen im Jahr 24 Stunden erreichbar sein. Daher müssen zwingend auch außerhalb der üblichen Bürozeiten Einsatzpläne verschiedener Mitarbeiter des Unternehmens erstellt werden, damit eine zügige Fallbearbeitung der Problemmeldung gewährleistet werden kann. Im Bedarfsfall wird von dieser Stelle aus die Krisenstabsleitung (zum Beispiel Bereichsvorstand, Geschäftsführer etc.) informiert. Die Krisenstabsleitung leitet sofort die entsprechenden Maßnahmen in die Wege. Wichtig ist hierbei, dass der Krisenstab Zugriff auf die aktuelle Mail- und Telefonliste der relevanten Bereiche und Stellen, sowohl intern als auch extern, hat.

Der Krisenstab bzw. das Krisenteam sollte nach Möglichkeit dauerhaft mit maximal fünf bis acht Personen besetzt werden. Es sollte durch das Krisenteam eine hohe Transparenz der Prozesse in allen Krisenbewältigungsphasen sichergestellt werden. Daher müssen aktuelle Informationen dem Team schnellst möglichst vorliegen, damit durch das Krisenteam alle weiterführenden strategischen und operativen Entscheidungen/Maßnahmen unverzüglich zentral gesteuert werden können (vgl. Glasl und Klindt 2012, S. 59 f.).

Das Krisenteam stellt somit sicher, dass notwendige Sofortmaßnahmen sofort nach dem Bekanntwerden eines Produktproblems ergriffen werden. Diese Sofortmaßnahmen werden als sogenannte „**First-Responder-Aktionen**“ bezeichnet. Sie sollen dazu dienen, dass auf mögliche Gefahren und Risiken, die durch ein fehlerhaftes Produkt entstehen können, von Beginn an positiv eingewirkt werden kann. Darüber hinaus soll auch die Außenwirkung, zum Beispiel durch die Medienberichterstattung, von Anfang an positiv beeinflusst werden. Daher ist es notwendig, dass nach dem Bekanntwerden möglicher Produktprobleme, das Krisenteam die Kommunikation (sowohl extern als auch intern) übernimmt. Hierzu sollten Sprecherrollen für interne und externe Kommunikation festgelegt werden. Im Falle eines Produktrückrufs überprüft das Krisenteam, ob die Medien, Behörden und andere externe oder interne Zielgruppen über die mögliche Fehlerhaftigkeit des Produkts bereits informiert wurden. Gegebenenfalls beantwortet das Krisenteam zudem fallbezogene Medien-, Kunden- oder Betroffenenanfragen. Wichtig ist zudem, dass Mitarbeiter mit einem direkten Kontakt nach außen, wie beispielsweise die Telefonzentrale oder die Pressestelle, vom Krisenteam hinsichtlich der Kommunikation unterwiesen werden. Darüber ist es wichtig, dass alle geplanten Kommunikations- und Marketingaktivitäten des Unternehmens überprüft und ggf. gestoppt werden (vgl. Glasl und Klindt 2012, S. 63 f.).

Neben den Sofortmaßnahmen bzg. der Kommunikation leitet das Krisenteam natürlich auch die im vorherigen Abschnitt beschriebenen Sofortmaßnahmen hinsichtlich eines Produktrückrufs ein.

Abschließend lässt sich festhalten, dass ein professionelles Krisenmanagement und eine gute Krisenkommunikation im Falle fehlerhafter Produkte, die möglicherweise die Gesundheit der Verbraucher beeinträchtigen können, von großer Bedeutung sind, um mögliche negative Auswirkungen auf das Unternehmen abzuwenden oder zu minimieren. Negative Folgen können materielle Auswirkungen sein, wie zum Beispiel Rückrufkosten, Umsatzeinbrüche, Verbraucherboykotte oder Verluste von Marktanteilen, oder immaterielle Auswirkungen, wie zum Beispiel Imageschäden oder eine langfristige Kundenabwanderung. Sie können somit im schlimmsten Fall eine Existenzbedrohung für das Unternehmen darstellen.

Gerade im Hinblick auf das gesteigerte mediale Engagement und den wachsenden Austausch von Verbrauchern über soziale Netzwerke wie Facebook oder Twitter ist ein professioneller Umgang mit Produktproblemen und eine schnelle Beseitigung dieser Probleme für ein Unternehmen zwingend erforderlich (vgl. Glasl und Klindt 2012, S. 12 ff.).

26.5 Qualitätssicherung

Die Qualitätssicherung dient dazu, schon während der Produktherstellung die Qualität des Produkts zu gewährleisten, damit eine Fehlerhaftigkeit des Produkts im Vorfeld verhindert wird.

Der Begriff „Qualitätssicherung“ umfasst alle organisatorischen und technischen Maßnahmen, die zur Sicherung der Produktqualität oder der Qualität einer Dienstleistung dienen. Wichtig ist hierbei, dass der Begriff „Qualität“ im Vorfeld durch das Unternehmen definiert wird (vgl. Voigt o. J.)“.

Im Bereich des Produktionsprozesses bedeutet der Begriff „Qualität die Erfüllung unternehmenseigener Produktspezifikationen“, wie zum Beispiel die Erfüllung der vom Kunden wahrgenommen Eigenschaften des Produkts oder die Erfüllung von Werksnormen. Das Erreichen dieser Qualität ist die Aufgabe des Qualitätsmanagements in einem Unternehmen. Laut der EN ISO 9000 Norm wird das Qualitätsmanagement als das Leiten und Lenken einer Organisation im Hinblick auf die Qualität der erzeugten Produkte oder angebotenen Dienstleistungen definiert. Das Qualitätsmanagement besteht dieser Norm zu Folge aus der Festlegung einer Qualitätspolitik und von Qualitätszielen, der Qualitätsplanung, der Qualitätslenkung, der Qualitätssicherung und einer Qualitätsverbesserung. Üblicherweise bildet das Unternehmen diese Funktionen in einem Qualitätsmanagementsystem ab.

Die Qualitätssicherung ist somit nur ein Teilbereich des Qualitätsmanagements und stellt eine zuverlässige Qualität von Produkten oder Dienstleistungen sicher. Das Kernelement der Qualitätssicherung ist hierbei die Prüfung, da durch Prüfungen zum Beispiel während des Produktionsprozesses die Produktqualität sichergestellt und zusätzlich ein Nachweis für eine erbrachte Qualität erzeugt wird. Darüber hinaus sind diese Prüfungsergebnisse ein Auslöser für Problemlösungsprozesse und können wichtige Impulse für den kontinuierlichen Verbesserungsprozess (KVP) liefern. Der kontinuierliche Verbesserungsprozess wird im Unternehmen etabliert, um den Produktionsprozess zu unterstützen und weiterzuentwickeln. Damit soll eine ständige Verbesserung der Qualität, Produktivität, Sicherheit etc. erzielt werden.

Während des Produktionsprozesses können trotz aller Bemühungen immer wieder Fehler auftreten. Aus diesem Grund es wichtig, dass das Unternehmen professionell mit diesen Fehlern umgeht. Hierzu ist die Etablierung eines Problemlösungsprozesses von Vorteil (vgl. Jung et al. 2013, S. 6 ff.).

Ist ein Problem bei der Produktion aufgetreten, ist es wichtig, dieses Problem zunächst zu beschreiben und abzugrenzen. Es ist hierbei wichtig zu klären, was für ein Fehler aufgetreten ist, wann der Fehler erkannt wurde, ob die Auswirkungen des Fehlers bereits beim Kunden sind, welche Teile und wie viele Produkte betroffen sind. Daraufhin werden Sofortmaßnahmen ergriffen, damit sämtliche fehlerhafte Teile aus dem Umlauf entfernt werden. Aus diesem Grund sollte eine Sortierprüfung in der gesamten Lieferkette des Unternehmens eingeführt werden. Anschließend werden die Ursachen der Fehlerhaftigkeit untersucht und Korrekturmaßnahmen festgelegt, die eine weitere Fehlerhaftigkeit des Produkts verhindern sollen. Diese Maßnahmen sollen im Produktionsprozess verankert und die Erkenntnisse auf andere bereits bestehende Prozesse oder auf zukünftige Produkte übertragen werden, um nachhaltig das Problem zu beseitigen (vgl. Jung et al. 2013, S. 97 ff.).

Abschließend ist es wichtig, die Wirksamkeit des im Unternehmen etablierten Qualitätssicherungssystems durch regelmäßig durchgeführte Audits zu überwachen und weiterzuentwickeln (vgl. Jung et al. 2013, S. 8).

Ein Qualitätssicherungssystem kann also dabei helfen, Produktfehler während des Produktionsprozesses frühzeitig zu erkennen und zu beseitigen. Dadurch kann ein Produktrückruf verhindert werden. Das finanzielle Risiko, das durch einen Rückruf des Produkts entsteht, kann somit minimiert werden. Zudem wird dadurch auch das Reputationsrisiko,

also die Gefahr als Unternehmen durch einen Produktrückruf mit großer medialer Aufmerksamkeit einen langfristigen Imageschaden und somit gravierende Umsatzeinbußen zu erleiden, verringert. Darüber hinaus sind auch regulatorische Folgen denkbar. Werden vermehrt gesundheitsgefährdende Produkte, wie bspw. bakterienverseuchte Lebensmittel, von einem Industriezweig in Umlauf gebracht, können durchaus von der Regierung schärfere Kontrollen verlangt bzw. angeordnet werden. Dies kann im Vorfeld durch ein bereits sehr gutes Qualitätssicherungsverfahren im Unternehmen vermieden werden.

26.6 Versicherungslösungen

Um die Folgen eines Produktrückrufs für ein Unternehmen zu mindern bzw. vollständig abzuwehren, besteht die Möglichkeit für das Unternehmen, im Vorfeld eine Produktschutz- oder Rückrufkostenversicherung abzuschließen. Dadurch kann das finanzielle Risiko für das Unternehmen begrenzt werden. Aber auch die Folgen einer negativen Medienberichterstattung können so (teilweise) abgesichert werden.

Welchen Schutz die einzelnen Versicherungslösungen im Fall eines Produktrückrufs bieten, wird im folgenden Abschnitt dargestellt. Jedoch bleibt zu beachten, dass das Unternehmen weiterhin ein hohes Reputationsrisiko trägt, da der eventuelle Imageschaden durch einen Produktrückruf nicht absehbar ist. Die Wirkung auf den Endverbraucher, also ob ein Produkt nach einem Produktrückruf überhaupt noch gekauft wird, kann nicht durch eine Versicherungslösung abgesichert werden.

26.6.1 Produktschutzversicherung

Bei der Produktschutzversicherung handelt es sich um eine spezielle Vermögensschadensversicherung. Ihren Ursprung hat sie in den USA. In Deutschland wurde die zunächst zaghafte gezeichnete Versicherung etwa Mitte der 1980er-Jahre eingeführt. Mittlerweile gibt es allerdings einige Versicherungsunternehmen, die diese spezielle Vermögensschadensversicherung anbieten.

Obwohl diese Versicherung für viele Unternehmen eine der wichtigsten Deckungen für selbst erlittene Vermögensschäden ist, führt die Produktschutzversicherung in der Versicherungsliteratur weithin ein Schattendasein. Durch ein fehlerhaftes oder gesundheitsgefährdendes Produkt können vor allem bei Herstellern und Lieferanten aus der Getränke-, Lebensmittel- und Kosmetikindustrie, aber auch bei Produzenten sonstiger Konsumgüter aus dem sogenannten „Non-Food-Sektor“ enorme Vermögensschäden entstehen. Diese Vermögensschäden können durch versehentliche Beeinträchtigungen im Produktherstellungsprozess aber auch durch vorsätzliche und böswillige Manipulation des Produkts oder Produkterpressung verursacht werden.

Um diese Risiken zu minimieren bzw. vollständig abzusichern, bietet die Produktschutzversicherung für das Unternehmen den besten Schutz. Gegenstand dieser Produkt-

schutzdeckung ist, dass der Versicherer dem Versicherungsnehmer, also dem Hersteller des Produkts, Versicherungsschutz gegen die Folgen von Produktmängeln und Produktmanipulationen gewährt. Dieser Versicherungsschutz umfasst die Kosten und Gewinneinbußen, die dem Versicherungsnehmer im Zusammenhang mit dem Produktmangel oder der Produktmanipulation entstanden sind. Darüber hinaus kann der Versicherungsnehmer auch die Übernahme weiterer Kosten im Rahmen der fakultativen Deckungserweiterung vereinbaren.

In der Produktschutzversicherung sind alle Produkte, einschließlich ihrer Bestandteile und Zutaten, versichert, die der Versicherungsnehmer herstellt, be- oder verarbeitet und verteilt. Zusätzlich sind auch die Produkte abgesichert, die von anderen Zulieferern unmittelbar oder mittelbar für den Versicherungsnehmer hergestellt werden. Die Voraussetzung für den Versicherungsschutz ist jedoch, dass die Produkte zum Zeitpunkt des Versicherungsfalles unter die im Versicherungsschein genannte Produktgattung fallen.

Die unterschiedlichen Versicherungsbedingungen der jeweiligen Versicherer knüpfen an verschiedene „Deckungsauslöser“ an. In der Regel sind dies die Tatbestände der versehentlichen Kontamination, vorsätzlichen Kontamination und der negativen Medienberichterstattung. Marktüblich werden hierfür die folgenden Definitionen verwendet:

- **Versehentliche Produktkontamination bzw. Produktmangel:** Droht durch eine Produktkontamination ein Personenschaden, besteht eine gesetzliche Verpflichtung zu einem Produktrückruf. Die drohende Schädigung von Personen und der damit verbundene Produktrückruf stellen hierbei den Deckungsauslöser dar. In allen Produktionsstadien, wie der Lagerung, der Auslieferung und auch in der Zuliefererkette, kann es zu unbeabsichtigten Beeinträchtigungen der Produkte kommen. Diese Beeinträchtigungen können beispielsweise durch Fremdkörper (zum Beispiel Glassplitter), Rückstände von Chemikalien (zum Beispiel Lösungsmittel) oder biologische Beeinträchtigungen (zum Beispiel Schimmelpilze) verursacht werden. Gemäß den Versicherungsbedingungen muss eine versehentliche Produktkontamination mit hinreichender Wahrscheinlichkeit durch einen ausreichenden Stichprobenbefund, sonstiger objektiven Tatsachen oder durch eine behördliche Anordnung festgestellt werden.
- **Vorsätzliche Produktkontamination:** Diese Form des Produktmangels liegt vor, wenn ein Dritte eine vorsätzliche, böswillige und rechtswidrige Veränderung des Produkts verursacht, behauptet oder androht. Diese Veränderung zielt darauf ab, die Gefahr von Personenschäden bei der Benutzung des Produktes herbeizuführen oder einen solchen Eindruck gegenüber der Öffentlichkeit zu erwecken. Eine vorsätzliche Produktkontamination umfasst sowohl die Produktsabotage als auch die Produkterpressung durch einen Dritten. Als Dritte wird hierbei jede natürliche Person einschließlich der Mitarbeiter des Unternehmens angesehen. Von dieser Bezeichnung sind jedoch folgende Personen des Unternehmens ausgeschlossen: Mitglieder eines geschäftsführenden Organs, gleichgestellte Generalbevollmächtigte, Gesellschafter von Personengesellschaften, Inhaber von Einzelfirmen und Insolvenz- und sonstige Vermögensverwalter. Diese Regelung gilt zudem für den entsprechenden Personenkreis bei ausländischen Gesellschaften.

- **Negative Medienberichterstattung:** Dies liegt vor, wenn das versicherte Produkt in der Medienberichterstattung zum Beispiel von Print- und Rundfunkmedien oder in einer Veröffentlichung einer Bundes- oder Landesregierung im Zusammenhang mit einem tatsächlichen oder behaupteten Produktmangel genannt wird. Gleches gilt im Zusammenhang mit einer Produktmanipulation.

Ist nun ein Versicherungsfall aufgrund der eben genannten Deckungsauslöser eingetroffen, ersetzt der Versicherer dem Versicherungsnehmer die folgenden Kosten, sofern diese angemessen und dem Versicherungsnehmer direkt und ausschließlich infolge des Versicherungsfalls entstanden sind:

- **Rückrufkosten:** Das sind die sogenannten Sofortkosten. Der Versicherer übernimmt hierbei die Kosten des Versicherungsnehmers für bestimmte Maßnahmen oder vergleichbare, kostengünstigere Ersatzmaßnahmen. Darunter fallen zum Beispiel die Kosten für die **Benachrichtigung von Endverbrauchern** und Kosten für Medienaufrufe. Zudem werden die Kosten für das **Vorsortieren und der Transport der betroffenen Produkte** erstattet. Oftmals muss für eine Rückrufaktion **zusätzliches Personal** eingesetzt werden. Auch diese Kosten werden vom Versicherer getragen. Darüber hinaus sind unter anderem auch die **Kosten für die Beseitigung oder Vernichtung** der fehlerhaften Produkte gedeckt.
- **Rehabilitationskosten:** Hierbei werden die Kosten des Versicherungsnehmers für Veröffentlichungen, zum Beispiel in **Fernsehwerbung**, übernommen, Mittels dieser Veröffentlichungen soll das Image des Versicherungsnehmers bzw. das Image des zurückgerufenen Produkts in der Öffentlichkeit wieder aufgewertet werden. Dies kann sich entweder in der Werbung für das betroffene Produkt oder für ein neues Produkt, das an die Stelle des betroffenen Produkts in den Markt eingeführt werden soll, ausdrücken.
- **Beratungskosten:** Hierzu zählen die Kosten für die **Einschaltung unabhängiger Sicherheits-, Werbe- oder Rückrufberater**, die nach Zustimmung des Versicherers zur Begrenzung der Folgen des Produktrückrufs hinzugezogen werden. Zusätzlich übernimmt der Versicherer die Kosten für erforderliche **Untersuchungen** zur Identifizierung der Ursachen des Produktmangels oder der Produktmanipulation.
- **Kosten für Beendigung einer Produktmanipulation:** Hierbei werden vom Versicherer die Personal- und Sachaufwendungen des Versicherungsnehmers für die Beendigung einer Manipulationsandrohung und/oder der Produktmanipulation erstattet.
- **Stornogebühren:** Der Versicherer übernimmt die Stornogebühren für geplante Werbekampagnen für ein versichertes Produkt, die aufgrund des Rückrufs nicht mehr durchgeführt werden (vgl. Klinkhammer 2014).

Der gesamte Eigenschaden des Versicherungsnehmers, der durch den Produktrückruf verursacht wurde, wird somit von der Produktschutzversicherung getragen. Der Hersteller wird dadurch nach dem Schadeneintritt wirtschaftlich so gestellt, als hätte es den Produktrückruf nie gegeben (vgl. Dogan 2017). Die Versicherung wird dadurch zu einem unver-

zichtbaren Schutz für produzierende Unternehmen, da ein Unternehmen jederzeit von einem Rückruf eines hergestellten Produkts betroffen sein kann.

26.6.2 Rückrufkostenversicherung

Neben der Produktschutzversicherung kann ein Unternehmen auch alternativ eine Rückrufkostenversicherung zur Absicherung der Risiken abschließen.

In der Betriebshaftpflichtversicherung (BHV) übernimmt der Versicherer keine Deckung für typische Überprüfungskosten, die bei einem Rückruf erforderlich sind. Darüber hinaus gibt es in der BHV bei einem Fremdrückruf einen Ausschluss von Ansprüchen bzgl. Kosten, die im Zusammenhang mit einem Rückruf geltend gemacht werden. Darunter fallen Aus- und Einbaukosten, die Nachbearbeitung, andere Schadenbeseitigung und weitere Vermögensnachteile wie Verbindungs-, Vermischungs-, Verarbeitungsschäden sowie Weiterver- und -bearbeitungsschäden (vgl. Röbe-Oltmanns und Schimikowski 2017, S. 123 ff.). Ein sogenannter Fremdrückruf liegt vor, wenn ein Dritter aufgrund eines fehlerhaften Produktteils zur Vermeidung von Personenschäden einen Rückruf durchführt (vgl. Rudkowski 2018). Dies liegt zum Beispiel dann vor, wenn ein Automobilhersteller die Airbags eines Zulieferers verbaut und aufgrund eines Produktfehlers der Airbags die hergestellten Fahrzeuge zurückrufen muss.

Da solche Fremdrückrufe in allen Branchen vorkommen können, ist es für den Hersteller wichtig, sich gegen dieses Risiko abzusichern. Die Rückrufkostenversicherung übernimmt im Rahmen eines Rückrufs zum Beispiel folgende Kosten:

- Benachrichtigungen, sowohl von Händlern, als auch von Verbrauchern (zum Beispiel durch Medienaufrufe),
- Vorsortierungskosten der vom Rückruf betroffenen Produkte,
- Produkttransport zu Sammelstellen oder Lieferanten,
- Zwischenlagerung der betroffenen Produkte,
- Austauschkosten der mangelhaften Produkte,
- falls kein Austausch vorgenommen wird, die Kosten für die Reparatur und Nachrüstungsmaßnahmen,
- Beseitigungs- und Vernichtungskosten,
- Kosten für die Ablauf- und Erfolgskontrolle der Rückrufaktion.

Es werden somit sowohl die Kosten für Eigen- als auch Fremdrückrufe gedeckt.

Darüber hinaus sind in der Rückrufkostenversicherung auch die Kosten für die Abwehr von Ansprüchen durch unberechtigt veranlasste Rückrufe durch Dritte gedeckt (vgl. Röbe-Oltmanns und Schimikowski 2017, S. 127 f.). Dieser Fall liegt vor, wenn das Produkt des Versicherungsnehmers von einem anderen Hersteller in einem Produkt verarbeitet wird, dieser Hersteller sein Produkt zurückruft und später einen Regressanspruch gegenüber dem Versicherungsnehmer geltend machen möchte, obwohl nicht das Produkt des Versi-

cherungsnehmers fehlerhaft war. Der Versicherungsnehmer ist in diesem Fall der Zulieferer.

In der Rückrufkostenversicherung werden allerdings keine Kosten für Ersatzlieferungen, Betriebsunterbrechung, Produktionsausfall, entgangenen Gewinn, Geldstrafen und Bußgelder übernommen. Zudem gibt es einen Ausschluss für Rückrufaktionen infolge von Produktmanipulation und Erpressung (vgl. Röbe-Oltmanns und Schimikowski 2017, S. 129 ff.). Der Ausschluss der Produktmanipulation und Erpressung stellt einen erheblichen Unterschied zu einer Produktschutzversicherung dar, da der Hersteller bzw. Zulieferer in dieser auch gegen solche Risiken abgesichert wird. Zudem werden in der Rückrufkostenversicherung keine Beratungskosten für Krisenberater etc. übernommen. Auch dies ist ein deutlicher Nachteil für den Versicherungsnehmer.

Es lässt sich somit zusammenfassend sagen, dass eine Rückrufkostenversicherung weitestgehend die Kosten einer Rückrufaktion übernimmt und der Versicherungsnehmer durch den Abschluss dieser Versicherung sein finanzielles Risiko minimieren kann. Allerdings bietet die Produktschutzversicherung einen deutlich höheren Versicherungsumfang, wodurch der Hersteller eines Produkts besser abgesichert ist.

26.7 Fazit

Von einem Produktrückruf können alle produzierenden Unternehmen betroffen sein. Wichtig ist es, dass der Rückruf des fehlerhaften Produkts professionell abgewickelt wird.

Dabei ist es vorteilhaft, wenn der Produkthersteller ein Rückrufmanagementsystem fest im Unternehmen integriert und die Kommunikation mit Medien, Behörden und Kunden zentral steuert. Nur eine professionelle und schnelle Abwicklung eines Rückrufs kann mögliche negative Folgen, wie Umsatzeinbrüche oder einen Imageschaden, reduzieren oder sogar verhindern.

Damit es erst gar nicht zu einem Produktrückruf kommt, ist es wichtig, ein Qualitäts sicherungssystem im Unternehmen zu etablieren. Dadurch können Produktfehler frühzeitig erkannt werden und das fehlerhafte Produkt gerät nicht in Umlauf.

Sollte trotz aller Vorkehrungen ein Produktrückruf unvermeidbar sein, decken die Produktschutzversicherung oder die Rückrufkostenversicherung Teile des finanziellen Risikos des Unternehmens ab. Wichtig ist hierbei, dass sich das Unternehmen im Vorfeld mit den unterschiedlichen Versicherungslösungen befasst und sich für die passende Versicherungsdeckung entscheidet. Nur so kann das Unternehmen das finanzielle Risiko, das durch einen Produktrückruf entsteht, minimieren.

Literatur

- Dogan, D. (2017). Wie Unternehmen den Albtraum eines Produktrückrufs überstehen. *Die VersicherungsPraxis*, 2017(9), 14–16.
- Glasl, T., & Klindt, T. (2012). *Krisenfall Produktrückrufe*. Stuttgart: Richard Boorberg.

- Heidemann, J. (2018). Kennen Sie schon RAPEX? *Die VersicherungsPraxis*, 2018(2), 19–22.
- Jung, B., Schweißer, S., & Wappis, J. (2013). *Qualitätssicherung im Produktionsprozess*. München: Carl Hanser.
- Klindt, T., & Wende, S. (2014). *Rückrufmanagement: Ein Leitfaden für die professionelle Abwicklung von Krisenfällen* (3. Aufl.). Berlin: Beuth.
- Klinkhammer, G. (2014). Die Produktschutzversicherung – Bedeutung, Zuschnitt, Markt (Teil 1). *Die VersicherungsPraxis*, 2014(4), 57–61.
- Poller, S. (2016). §2 Allgemeine deliktische Ansprüche, §§ 823 ff BGB. In Kroiß (Hrsg.) Roth: *Formularbibliothek Zivilprozess – Verkehrsrecht, Teil 2* (3. Aufl., Rn 99–125.). Baden-Baden: Nomos Verlagsgesellschaft.
- Produktrückrufe. (2019a). Tückische Gefahr: Aldi Nord informiert zu möglichen Glassplittern in Sölde Hähnchenschnitzeln. <http://produktrueckrufe.de/nahrungsmittel-und-genussmittel/1371-aldinord-rueckruf-haehnchenschnitzel>. Zugegriffen am 29.07.2019.
- Produktrückrufe. (2019b). Erneut Verdacht auf Kolibakterien (VTEC) in Iglo Petersilie (TK): Vor dem Verzehr wird gewarnt. <http://www.produktrueckrufe.de/nahrungsmittel-und-genussmittel/1369-iglo-rueckruf-petersilie2>. Zugegriffen am 29.07.2019.
- Produktwarnungen. (2019a). Rückruf: Erstickungsgefahr – Flying Tiger ruft Holzeisenbahn zurück. <https://www.productwarnung.eu/2019/03/26/rueckruf-erstickungsfeahr-flying-tiger-ruft-holzeisenbahn-zurueck/13179>. Zugegriffen am 29.07.2019.
- Produktwarnungen. (2019b). Rückruf: Erstickungsgefahr bei verschiedenen Seek O'Blocks Konstruktionsspielzeugen. <https://www.productwarnung.eu/2019/04/23/rueckruf-erstickungsgefahr-bei-verschiedenen-seeko-blocks-konstruktionsspielzeugen/13620>. Zugegriffen am 29.07.2019.
- Produktwarnungen. (2019c). Rückruf: E.Coli – Hersteller Lincet ruft Chauorce Käse zurück. <https://www.productwarnung.eu/2019/05/10/rueckruf-e-coli-hersteller-lincet-ruft-chaource-kaese-zurueck/13775>. Zugegriffen am 29.07.2019.
- Röbe-Oltmanns, H., & Schimikowski, P. (2017). *Seminar zum Thema: Gewerbliche und industrielle Haftpflichtversicherung*. Münchner Seminar für Wirtschafts- und Versicherungsrecht GmbH.
- Rudkowski, L. (2018). Aktuelle Herausforderungen für die Rückrufkostenhaftpflichtversicherung. VersR online. <http://www.versr.de/aufsatzen/len-a-rudkowski-aktuelle-herausforderungen-fuer-die-rueckrufkostenhaftpflichtversicherung/>. Zugegriffen am 29.07.2019.
- Spiegel Online. (2019a). BMW ruft 480.000 Fahrzeuge zur Airbag-Kontrolle zurück. <https://www.spiegel.de/auto/aktuell/bmw-ruft-480-000-autos-wegen-airbag-kontrolle-zurueck-a-1252832.html>. Zugegriffen am 20.07.2019.
- Spiegel Online. (2019b). Volvo muss eine halbe Million Autos nachrüsten. <https://www.spiegel.de/auto/aktuell/volvo-muss-eine-halbe-million-autos-wegen-brandgefahr-nachruesten-a-1278288.html>. Zugegriffen am 29.07.2019.
- Voigt, K.-I. (o. J.). *Qualitätssicherung*. Gabler Wirtschaftslexikon. <https://wirtschaftslexikon.gabler.de/definition/qualitaetssicherung-44396>. Zugegriffen am 29.07.2019.
- Zeit Online. (2019). Deutschlandweiter Rückruf von belasteter Milch. <https://www.zeit.de/wirtschaft/2019-10/bakterien-milch-rueckruf-supermaerktegesundheitsrisiko>. Zugegriffen am 18.12.2019.

Herr Christian Kuhrt ist Geschäftsführer der DMK Versicherungskontor GmbH, dem firmenverbundenen Vermittler der Deutschen Milchkontor GmbH (DMK), deren Molkereiprodukte unter anderem unter den Marken Milram und Oldenburger bekannt sind. In dieser Funktion blickt er auf über zehn Jahre Erfahrung in allen Sparten der industriellen Versicherung sowie Financial Lines zurück. Vor seiner beruflichen Tätigkeit für DMK Versicherungskontor GmbH arbeitete er fast 15 Jahre für seinen Ausbildungsbetrieb, den Versicherungsmakler C. Wuppessahl, später Jaspers Wuppessahl und war nachfolgend fünf Jahre als Prokurist für Lübcke Bremen GmbH und deren Altersversorgungsgeellschaft LC-GA tätig. Neben seiner Expertise in nahezu allen Sparten der industriellen Sach-,

Haftpflicht und Personenversicherungen umfasst sein Spektrum zudem Spezialkenntnisse auf den Gebieten der Transport-, Kredit- und Produktschutzversicherung. Herr Kuhrt ist Versicherungsfachwirt und hat nachfolgend bei der Deutschen Versicherungsakademie - Studienort Hamburg - mit seiner Abschlussarbeit zum Riskmanagement in der Güter-Transport-Versicherung bei Prof. Walter Karten den Titel Versicherungsbetriebswirt (DVA) erworben.

Monique Neußmann absolvierte eine Ausbildung zur Sozialversicherungsfachangestellten bei der AOK Rheinland/Hamburg. Im Anschluss studierte sie Versicherungswesen mit den Schwerpunkten Risikomanagement, Bilanzierung sowie Haftpflicht-/Unfall-/Kraftfahrt und Rechtsschutzversicherung am Institut für Versicherungswesen der Technischen Hochschule Köln. Zuletzt absolvierte sie dort auch das Masterstudium Risk & Insurance.



Naturgefahren

27

Malwine Tewes und Andrea Scholtes

Zusammenfassung

Naturgefahren treten schon seit Anbeginn unserer Zeit auf und verwirklichen sich auf vielseitige Art und Weise. Trotz weitentwickelter Technologien, wie Frühwarnsysteme oder besondere Bauweisen, stellen Naturgefahren nach wie vor eine große Gefahr dar und können zur Bedrohung für Menschen, Umwelt, Sach- und Vermögenswerte führen. In vielen Fällen treten Naturgefahren unvorhergesehen oder mit kurzen Vorwarnzeiten auf, daher kann das Schadenausmaß aufgrund der Vielzahl von Betroffenen in exponentiellen Gebieten sowie von Wertekonzentrationen im industriellen Bereich sehr hoch ausfallen. Neben Präventionsmaßnahmen ist eine Absicherung von Naturgefahren durch den Einkauf von Versicherungsschutz sowohl für Industrieunternehmen als auch für Privatpersonen zur Risikoabsicherung im Versicherungsfall bzw. zum Erhalt eines Schadenausgleichs sinnvoll. Selbst ein dokumentierter und vorab getester Notfallplan kann die Auswirkungen von Naturereignissen nur vermindern, jedoch können diese nicht vollständig vermeiden werden. Mehrere Faktoren, wie zum Beispiel der Klimawandel, tragen dazu bei, dass die Schadenserwartungen aufgrund der Intensität und Häufigkeit wetterbedingter Naturgefahren verstärkt werden. Deshalb, aber auch wegen zunehmender Industrieverdichtung, muss in Zukunft vermehrt mit höheren Frequenzen und größeren Schäden gerechnet werden. Vorsorgemaßnahmen müssen aufrechterhalten und an die sich ändernden Gegebenheiten angepasst werden.

M. Tewes (✉)

FM Insurance Europe S. A., Frankfurt, Deutschland

E-Mail: malwine.tewes@fmglobal.com

A. Scholtes

TH Köln, Institut für Versicherungswesen, Köln, Deutschland

E-Mail: andrea.kittner@mailbox.org

27.1 Einleitung

Naturgefahren sind in den letzten Jahren verstkt in den Fokus einer breiteren ffentlichkeit gerkt, unter anderem da sich die Schden, im Vergleich zur Situation der letzten Jahrzehnte, durch extreme Wetterereignisse in dicht besiedelten und stetig wachsenden Ballungszentren signifikant erhht haben. In Verbindung mit dem in den Medien viel diskutierten Phnomen „Klimawandel“ und den daraus resultierenden prognostizierten Langzeitfolgen werden extreme Naturereignisse wie tropische Strme, Waldbrnde, Drren und berschwemmungen strkter als zuvor wahrgenommen.

Im Folgenden werden unter anderem die Ursachen, Auswirkungen sowie der Umgang mit Naturgefahren beschrieben, wobei der Fokus auf berschwemmungseignissen liegt, die beispielhaft anhand eines Schadenereignisses aus der Industrie aufgezeigt werden.

Einen berblick ber Naturgefahren, die im Jahr 2017 stattgefunden haben, gibt Abb. 27.1. Jeder Punkt steht hierbei fr ein Naturgefahrenereignis, wobei die grtzen Punkte die 20 grtzen Ereignisse des Jahres 2017 anzeigen. Insgesamt haben sich im Jahr 2017 etwas mehr als 700 Naturgefahren als Schadenereignis ausgebildet. Diese sind nach ihrer Art, aber auch nach den Ausmaen berall auf der Welt verteilt. Vor allem aber sind die mittleren Breitengrade betroffen, die durch eine starke Besiedlung und industrielle sowie landwirtschaftliche Aktivitt gekennzeichnet sind. Zu erkennen ist, dass Tsunamis, Erdbeben und vulkanische Aktivitten vor allem an der Westkste Nordamerikas und in Asien auftreten, im Wesentlichen entlang der globalen tektonischen Bruchzonen. Sturmfluten treten weltweit als Kombination von Starkwind, Gezeitenhochstand und Wellenschlag auf, sind aber auf Ksten- oder Mndungsgebiete beschrkt. Naturgefahren, die mit extremer Hitze und daraus folgenden Waldbrnde oder Drren einhergehen, sind ebenfalls global verteilt, allerdings waren die Westkste der USA und der Sden Europas im Jahr 2017 besonders stark betroffen. Prgend fr das Jahr 2017 waren die Hurrikane-Sturmereignisse vor allem an der Ostkste der USA. In Verbindung mit erheblichen Niederschgen fanden dort vier der 20 grtzen Ereignisse statt. berschwemmungen hingegen sind weniger zentriert, sondern treten nahezu berall auf der Welt auf, einerseits als Flusshochwasser, andererseits durch ortsunabhngigen Starkregen.

Die Ursache von Naturgefahrenereignissen, wie der Mensch mit diesen Gefahren umgehen kann und welche Vorsorgemanahmen getroffen werden knnen, wird im Folgenden beschrieben.

27.2 berblick ber Naturgefahren

Eine Naturgefahr ist ein durch natrliche Prozesse ausgelster Zustand oder Vorgang, der Schden verursachen oder Opfer fordern kann. Das Risiko ist das Ma fr die Wahrscheinlichkeit, dass durch den natrlich ausgelten Prozess tatschlich ein Schaden entsteht. Entsprechend schliet das Risiko zwei unabhngig voneinander zu ermittelnde Faktoren

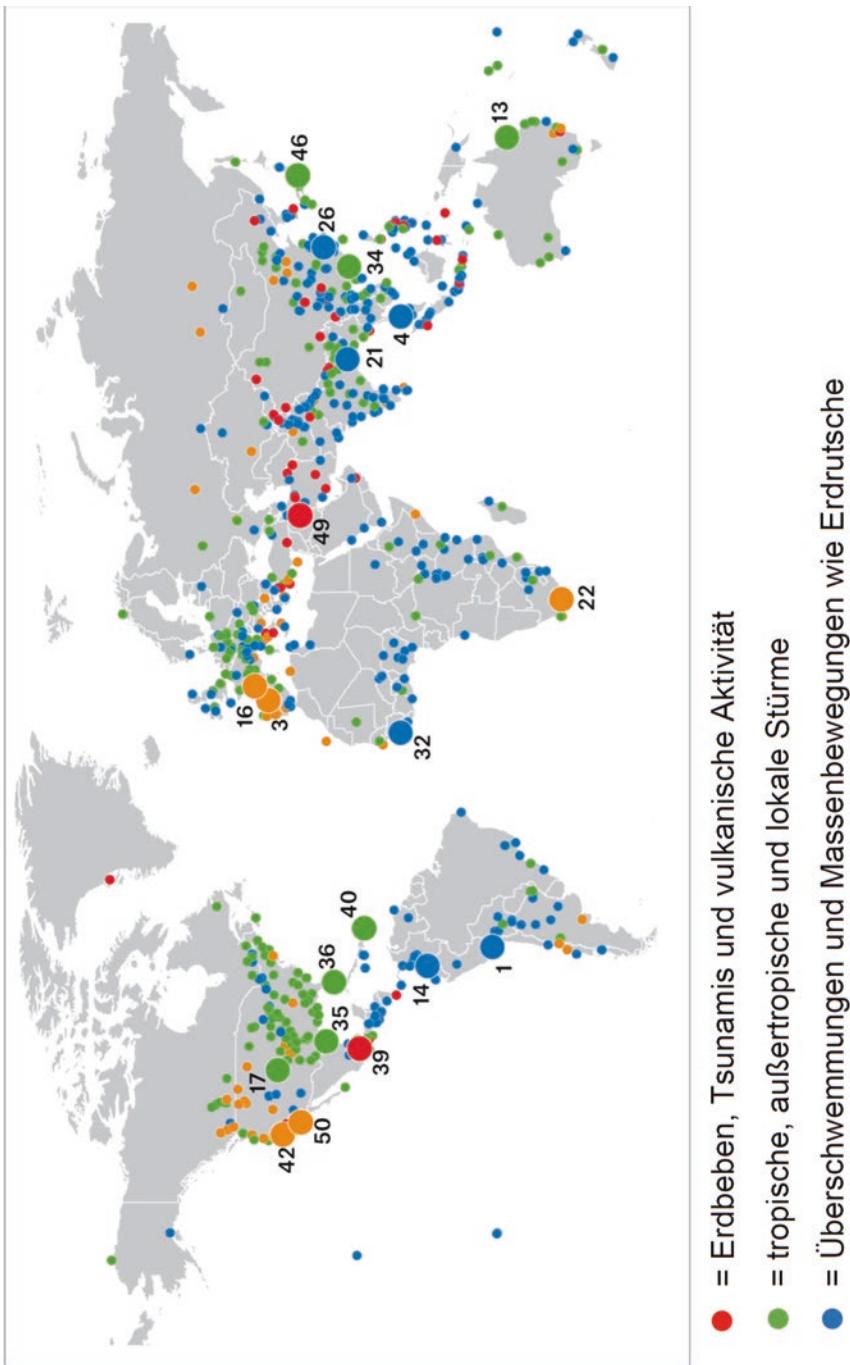


Abb. 27.1 Übersicht der Naturgefahrenereignisse im Jahr 2017. (Quelle: Munich Re 2018, S. 66)

Tab. 27.1 Übersicht der Naturgefahren. (Quelle: eigene Darstellung)

Endogen / Tektonisch	Gravitorisch	Klimatisch	Sonstige
Erdbeben	Lawinen	Überschwemmungen	Meteoriteneinschläge
Vulkanausbruch	Erdrutsche	Tropische Wirbelstürme	Schädlingsplagen
Tsunamis		Tornados	
		Dürren	
		Hagel	

ein, einerseits die Eintrittshäufigkeit der Naturgefahr in einer bestimmten Region, andererseits das mögliche Ausmaß der davon verursachten Schäden.

Naturgefahren können entweder auf endogene oder exogene Ursachen zurückgeführt werden. Endogene Ursachen haben ihren Ursprung im Erdinneren. Hierzu zählen zum Beispiel Erdbeben oder Vulkanausbrüche, während exogene Naturereignisse von außen auf die Erdoberfläche einwirken. Stürme, Starkregen oder extreme Temperaturen sind Beispiele für exogene Ereignisse, welche unter anderem in Dürren oder auch Hochwasser resultieren können.

Eine Naturgefahr ist ein potenzielles Schadeneignis. Zu einer Naturkatastrophe wird es erst, sobald sich die Gefahr verwirklicht hat und ein wirtschaftlicher oder humanitärer Schaden entstanden ist.

Aus dieser Begriffsbestimmung folgt, dass die Grundlage für eine Naturkatastrophe das resultierende Schadenpotenzial ist, und es entsteht folglich im Konfliktbereich zwischen dem natürlichen und dem humanen System (vgl. Dikau und Voss 2000). Beispielhaft sei hier die San Francisco Bay Area erwähnt, welche einen hohen wirtschaftlichen und kulturellen Anreiz zur Erschließung bietet und daher trotz des Wissens um eine stark exponierte Naturgefahrenlage dicht besiedelt ist.

Tab. 27.1 zeigt eine tabellarische Übersicht der Naturgefahren, unterteilt nach ihren Oberklassen.

27.3 Spezialisierung: Überschwemmung durch Hochwasser

Hochwasser entsteht, wenn Gewässer über ihre Ufer treten und Schäden verursachen, zum Beispiel durch einen erhöhten Wasserstand, die kinetische Energie von Wasser und Treibgut oder durch Eintrag von Chemikalien und Schmutzpartikeln. Im Folgenden werden nur Überschwemmungen durch Hochwasser beschrieben, da rund ein Drittel aller weltweiten Naturgefahrenereignisse auf ein Hochwasser zurückzuführen sind.

Faktoren, die Hochwasser begünstigen, sind unter anderem die Schneeschmelze im Frühjahr, ausgedörrte Böden im Hochsommer, aber auch die Uferform, Bodenbeschaffenheit und Topologie haben Einfluss auf das Auftreten. Gerade wenn mehrere Effekte gleichzeitig auftreten, begünstigt dies Naturkatastrophen, so zum Beispiel anlässlich des Juni-

hochwassers von 2013 in Mitteleuropa. Dort hatte es bereits im Monat Mai viel geregnet, sodass die Bodenfeuchte sehr hoch war und kein weiteres Wasser mehr aufgenommen werden konnte. Im Juni zog ein weiteres Tiefdruckgebiet über das Land. Dies hatte zur Folge, dass innerhalb von vier Tagen bis zu 400 Millimeter Niederschlag gemessen wurden. Da der Boden gesättigt war, ist der größte Teil des Niederschlags direkt in die Flüsse gelaufen, sodass die Pegel stark angestiegen sind. Hierbei wurden zahlreiche Städte überschwemmt und es entstand allein in Deutschland ein Schaden in Höhe von über sechs Milliarden Euro. Insgesamt handelte es sich um ein Jahrhunderthochwasser, also um ein Ereignis, welches statistisch gesehen nur einmal in 100 Jahren überschritten werden sollte (vgl. Podbregar und Lohmann 2015, S. 193 ff.). In Passau wurde sogar ein Rekordpegelstand der Donau von 12,89 Metern gemessen, sodass dort so schwere Überschwemmungen ausgelöst wurden, wie dies zuletzt vor 500 Jahren der Fall war. Durch das Bevölkerungswachstum und die starke Besiedlung von Küsten und flussnahen Gebieten werden in Zukunft mehr Menschen von Hochwasser betroffen sein. Auch Industriebetriebe siedeln sich vermehrt in der Nähe von Häfen oder Gewässern an, wodurch das Schadenpotenzial für sie steigt. Aber auch durch den steigenden Meeresspiegel, die intensive Nutzung von Überschwemmungsflächen der Flüsse, die Versiegelung der Bodenfläche durch den Ausbau der Infrastruktur (Straßen, Häuser etc.) und die voranschreitende Industrialisierung kann das überschüssige Wasser nicht auf ursprünglichem Weg abfließen, sodass das Überschwemmungsrisiko gestiegen ist. Flussverkürzungen und -begradigungen, wie zum Beispiel des Rheins, führen dazu, dass das Gefälle höher ist und das Wasser somit schneller fließt. So wurden Ober- und Niederrhein insgesamt um über 100 Kilometer verkürzt, sodass eine Hochwasserwelle im Vergleich zur Mitte des 20. Jahrhunderts nur noch 25 Stunden anstatt knapp 65 Stunden benötigt, um von Basel nach Karlsruhe zu gelangen. Dadurch verkürzt sich die Vorwarnzeit stark und es bleibt weniger Zeit für Gegenmaßnahmen. Denn es gilt: Je länger die Vorwarnzeit ist, desto besser greifen entsprechende Maßnahmen zur Schadenverhütung. Auch Böden und Wälder können große Teile des Wassers abfangen. Allerdings hat auch hier der Mensch durch den Straßenbau und die Besiedlung eingegriffen, sodass dieser natürliche Puffer weitestgehend wegfällt. Durch modernere Landwirtschaft mit schweren Maschinen wird der Boden stark verdichtet und kann weniger Wasser aufnehmen, als es vor einigen Jahrzehnten der Fall war. Hinzu kommt die globale Erwärmung, welche die Gletscher abtauen und den Meeresspiegel steigen lässt, sowie Starkregen und Stürme begünstigt, sodass in Zukunft mit noch größeren Überschwemmungskatastrophen gerechnet werden muss (vgl. Podbregar und Lohmann 2015, S. 199 f.).

27.3.1 Schadenbeispiel: Betriebsunterbrechung durch Hochwasser bei einem Schienenfahrzeughersteller

Eine Produktionsstätte eines führenden Bahn- und Straßenbahnherstellers befindet sich am Oberlauf eines Flusses, getrennt durch einen Deich. Durch Dauerregen hatten sich im

Hochsommer die Wassermassen des Flusses vervielfacht. Während normalerweise rund zehn Kubikmetern Wasser pro Sekunde durch den Fluss fließen, wurden in diesen Tagen mehr als 160 Kubikmeter pro Sekunde von den Messstellen festgestellt. Der Pegel des Flusses lag anstatt von 80 Zentimetern bei 3,40 Metern Höhe und erreichte ein Abflussmaximum, welches ein 500-jährliches Hochwasser bei weitem überschritt. 20 Minuten nach der offiziellen Hochwasserwarnung der lokalen Feuerwehr erreichte der Fluss entlang des Werksgeländes an zwei Stellen die Deichkrone, kurz danach gab der Deich an einer Stelle nach, wodurch das Werk überflutet wurde. In kürzester Zeit standen mehr als 90.000 Quadratmeter überdachte Fläche unter Wasser.

Aufgrund der Nähe zum Gewässer und den damit verbundenen Gefährdungen existierte ein Hochwassernotfallplan, um Schäden und Betriebsunterbrechungen möglichst zu vermeiden bzw. nachhaltig zu vermindern. Die Wassermassen sowie die Schnelligkeit des Eintreffens hatten den Standort trotz existierendem Notfallplan überrascht. Anders als zum Beispiel Anlieger des Niederrheins, denen wegen einer meist recht zuverlässigen Prognose des Hochwasserkamms mehrere Stunden oder sogar Tage zur Vorbereitung und für Abwehrmaßnahmen bleiben, gab es in diesem Fall eine Vorlaufzeit von unter einer Stunde. Ausschlaggebend war hierbei die geringe Entfernung zur Quelle des Flusses und der Tatsache, dass sich insbesondere Oberflächenwasser aufgrund von extremen Regenfällen schnell gesammelt hatte.

Der Notfallplan umfasste zum Beispiel das Füllen von Sandsäcken und deren Platzieren an möglichen Wassereintrittsstellen, das Sichern von Geräten und Maschinen, insbesondere bei produktionsrelevanten Anlagen, und das Umlagern besonders hochwertiger oder aufgrund langer Lieferzeit kritischer Bestände. Im beschriebenen Schadenfall waren jedoch innerhalb kürzester Zeit nicht nur tiefergelegte Bereiche, Wartungsgruben und Kellerräume vollgelaufen, sondern der komplette Standort stand 1,70 Meter unter Wasser.

Ein erster Rundgang durch das gesamte Außengelände und die Produktionshallen zeigte das volle Schadensausmaß. Sämtliche Testgleise zur Überprüfung des dynamischen Fahrverhaltens waren vollständig mit Schlamm und Geröll überdeckt, übergabefertige Bahnen im Fahrzeuginneren bis zur Höhe der Sitzpolster beschädigt und es wurden enorme Schäden an den großen Rolltoren und Außenwänden festgestellt.

In den ersten Stunden errichteten über 100 Helfer des THW einen temporären Deichschutz mit Sandsäcken und stellten eine erste Notstromversorgung her.

Auch wenn das Hochwasser bereits über Nacht wieder zurückging, war ein massiver Schaden innerhalb der Produktionshallen entstanden. An den Wänden, den Wagenkästen, den fertigen Fahrzeugen sowie den Sicherungskästen, Maschinen und Lagerbereichen zeichnete sich klar die Hochwasserlinie ab. Unterhalb der Hochwassermarken war alles matschig und feucht, oberhalb gab es auf den ersten Blick keinerlei Schadensanzeichen. So war zum Beispiel eine Lackierkabine und deren Steuerungseinheit betroffen, jedoch nicht die horizontal schwebend fertig lackierten Teile an der Förderkette.

Das Hochwasser hatte sämtliche produktionsrelevante Maschinen mit Schlamm überzogen, mehrere hundert Handschweißgeräte sowie jeden einzelnen Werkzeugkasten. Sämtliche Hallen, alle Geräte, Werkzeuge und Material bis zur kleinsten Schraube mussten

gereinigt oder entsorgt werden. Halbfertige Fahrzeuge, die auf Hebebühnen standen, schienen auf den ersten Blick nicht beschädigt worden zu sein. Später stellte sich aber heraus, dass herabhängende Kabelstränge wegen des Kapillareffektes Wasser ansogen. Alle Kabelstränge mussten daher demontiert und ersetzt werden.

Als erste Minimierungsschritte lag der Fokus in den ersten Tagen auf der Beseitigung des Schlammes sowie der Geröllmassen. Die Oberflächen der Maschinen wurden grob von Schlamm befreit, um eine bessere Zugänglichkeit bzw. Bemusterung zu gewährleisten. Hierbei war es zum Teil erforderlich, die Schlammablagerungen wieder zu nassen, um eine stärkere Verkrustung zu vermeiden. Erst nach dieser Grob- und sich daran anschließender Feinreinigung konnten die eigentlichen Sanierungs- und Konservierungsmaßnahmen in Angriff genommen werden. Hierbei war insbesondere eine rasche Priorisierung der zu reinigenden Maschinen und Anlagen wichtig, basierend auf Faktoren wie zum Beispiel Dringlichkeit des Auftrages, der prognostizierten Auslastung der betroffenen Maschinen, der Möglichkeiten der Wiedereingliederung in die Produktionsstraße oder Überlegungen, ob alle Produktionsschritte intern bewältigt oder extern vergeben werden konnten.

Im Verlauf der ersten Wochen konnten rund 50 Prozent aller Materialschäden kategorisiert werden. In der Frühphase, also während des Entschlammens und anschließenden Grobreinigens, wurde mit bis zu 200 Hochdruckwaschgeräten und Dampfstrahlern gearbeitet. In sechs großen Ultraschallbädern wurden vorsortierte Kleinteile wie Schrauben und Muttern innerhalb eines Monates gereinigt. Alle Gebäudeflächen wurden bis zur Wasserlinie grob vorgereinigt, Trockenbauelemente wurden unter Erhalt der Ständerwerkskonstruktion demontiert und es wurden Dämmungen entfernt. An Massivwänden wurde Putz abgeschlagen, um die sonst unvermeidbare Schimmelausbildung zu stoppen.

Den größten Teil der Arbeiten hat ein speziell dafür beauftragtes Sanierungsunternehmen übernommen. Ein zeitkritischer Bereich befand sich im Archiv im Keller. Hunderte wasserdurchtränkte und zum Teil verklebte Aktenordner konnten geborgen und durch ein Gefriertrocknungsverfahren gesichert werden. Nach einer ersten Selektion der Dokumentationsordner wurden diese kartonweise in Folien eingeschweißt, nahezu luftdicht verpackt und in einem Kühltransport zur weiteren Verarbeitung in einzelnen Chargen zu einen Vakuum-Gefriertrocknungsprozess zugeführt. Nach dem abgeschlossenen Trocknungsprozess, der etwa einen Monat dauerte, konnten die jeweiligen Dokumente wieder verpackt und unter Beigabe der ursprünglichen Identifizierungsmerkmale an den Standort zurückgesandt werden.

Im Nachgang des Schadenfalls wurde das Archiv in die oberen Etagen verlegt. Ferner wurde ein Spreepegelmesser auf Höhe des Standortes installiert und die Pegeldaten direkt an die Wache übermittelt. Selbst geringe Schwankungen und rasche Ansteige der Spree können nun beobachtet werden, um entsprechende Maßnahmen zu ergreifen.

Schon ein Jahr nach dem Schaden wurde eine Hochwasserspundwand zwischen Spree und Werksgelände fertig gestellt, wodurch schon im kommenden Jahr bei ähnlicher Durchflussmenge und ähnlichem Wasserstand eine erneute Betriebsunterbrechung vermieden werden konnte, da die Wassermassen vom Betriebsgelände ferngehalten werden konnten.

27.3.2 Evaluierung hochwasserexponierter Standorte

Um einen hochwasserexponierten Standort bewerten zu können, spielen neben der Lage, also der Einstufung in eine Hochwasserzone, die Bauweise sowie die Belegungsart des Gebäudes eine entscheidende Rolle. Neben der Geschossanzahl ist es auch entscheidend, welche Einrichtungen sich in welchem Stockwerk befinden. So sollten sich prozesskritische Anlagen, zum Beispiel die Hydraulikaggregate eines Stahlherstellers, Elektroversorgungen oder auch Archive, nicht im Keller befinden, um mögliche Schäden an wichtigen Geräten von vorn herein zu vermeiden.

Bei der Bauweise kommt es darauf an, welche Materialien (zum Beispiel Stein, Holz, Mineralwolle oder Polyurethan als Dämmmaterial) verbaut wurden und wie anfällig diese auf ein mögliches Hochwasserszenario reagieren.

Beim Aufbau der Außenwände kommen unterschiedliche Dämmstoffe zur Anwendung. Diese können als Schicht vor oder an die tragende Wandstruktur befestigt werden. Ebenso ist es möglich, dass die Wärmedämmung als Sandwichpaneel das Dämmmaterial in seinem Aufbau fest integriert. Hierbei sind die Deckschichten meistens aus Metall und der Kern aus mineralischen Fasern oder mehr oder weniger stark geschäumten Kunststoffen. Der Dämmstoff aus Fasern ist in der Regel nicht brennbar, allerdings nimmt er Wasser auf und muss nach einem Hochwasser aufwändig getrocknet werden. Polyurethan oder ähnliche Schäume eignen sich besser für die Gefahr Hochwasser, allerdings sind diese Materialien brennbar, werden meistens aber als schwer entflammbar bezeichnet.

Neben dem Gebäude an sich muss auch die Umgebung geprüft werden. Hierbei ist darauf zu achten, ob beispielsweise ein Gefälle vorhanden ist, sowie auf die jeweilige Bodenbeschaffenheit, um die Fließrichtung und -geschwindigkeit des Wassers zu bestimmen. Außerdem ist zu evaluieren, ob im Hochwasserfall Verunreinigungen oder potenzielles Treibgut, wie verunreinigter Schlamm, Baumstämme, Dünger oder benachbarte Lagergüter, mit dem Wasser transportiert werden. Gerade bei Klärwerken oder Industrien mit gefährlichen Stoffen, wie zum Beispiel Öllagerungen, gilt besondere Vorsicht, da hier neben der Gefährdung von betroffenen Standorten zusätzlich ein erhöhtes Umweltrisiko bestehen kann.

Die Einstufung in eine Hochwasserzone erfolgt durch die Schadeneintrittswahrscheinlichkeit und die möglichen Schadenausmaße eines bestimmten Risikos. So werden zum Beispiel Standorte in weniger, in moderat (alle 500 Jahre Eintrittswahrscheinlichkeit) oder in hoch (alle 100 Jahre) exponierte Überschwemmungsgebiete unterteilt. Auch bei schwach exponierten Standorten kann Hochwasser durch Starkregen entstehen, sodass geprüft werden muss, in welche Richtung und ob das Wasser abfließt und wo es zu Überschwemmungsbereichen kommen kann.

Um all diese Faktoren erfassen zu können, wird im Regelfall neben der theoretischen Hochwasserbestimmung anhand von Kartenmaterial eine Vor-Ort-Besichtigung eines hochwasserexponierten Standortes durchgeführt, um das Schadenpotenzial detaillierter zu

bestimmen. Eine solche Vor-Ort-Besichtigung wird bei Standorten mit hohem Gesamtversicherungswert immer durchgeführt. Jedoch werden auch kleinere Standorte besichtigt, wenn dort mehrere Faktoren zusammentreffen oder Besonderheiten bestehen und dadurch ein erhöhtes Risiko vorhanden ist. Das Schadenpotenzial wird durch den Prozentanteil vom Gesamtschaden sowie daraus resultierenden Betriebsunterbrechungszeiten ausgedrückt.

Zur ersten Bestimmung des Risikos dienen Hochwasserkarten, welche von verschiedenen Anbietern bereitgestellt werden. Diese werden unter anderem vom Gesamtverband der Deutschen Versicherungswirtschaft GdV (Zonierungssystem für Überschwemmung, Rückstau und Starkregen; ZÜRS), der SwissRe oder von lokalen Landesbehörden bereitgestellt. Andere Systeme greifen auf die Daten der lokalen Behörden zurück und geben teilweise nur Zonierungen in Hochwasserbereiche an. Bei einzelnen großen Standorten bieten sich die lokalen Karten der Landesbehörden an, da gerade die Höhe der Überschwemmung ein entscheidender Faktor ist.

Eine weitere Hilfe stellt die Zusammenarbeit mit Wasserbaubehörden dar, welche vor Ort eine Einschätzung über das Hochwasserrisiko und den errichteten Hochwasserschutzbauten abgeben können.

27.3.3 Quantifizierung von Schadenserwartungen

Die Quantifizierung von Schadenserwartungen bei gefährdeten Standorten wird durch eine Risikobewertung vor Ort durchgeführt. Wenn dies nicht möglich ist, wird mithilfe von Satellitenfotos, topografischen Karten und expliziten Hochwasserkarten eine Einschätzung der Hochwassergefährdung vom Schreibtisch aus vorgenommen. Insbesondere bei prozesskritischen Maschinen und Anlagen ist es wichtig zu wissen, auf welchem Höhenniveau diese errichtet sind. Ein besonderes Augenmerk sollte hierbei auf Antrieben und Schaltanlagen liegen. Zur Vermeidung von Wasserschäden bei kleineren Wasseransammlungen befinden sich diese vorzugsweise oberhalb von 30 cm über dem Boden. Ferner sollte Lagergut zumindest auf Paletten, bestenfalls auf höheren Regallagerebenen gelagert sein. Ein weiterer Faktor ist, wie feuchtigkeitsbeständig die Ware ist, da bei einer hohen Luftfeuchtigkeit auch höhergelegene Produkte betroffen sein können (zum Beispiel Aufweichen von Kartonagen). Gerade bei elektrischen Komponenten, wie zum Beispiel integrierten Schaltkreisen, kann Feuchtigkeit zu Korrosion und damit erhöhten Schäden führen. Auch in der Nahrungsmittelproduktion oder in pharmazeutischen Unternehmen ist die Beseitigung von Überschwemmungsschäden mit einem hohen Aufwand verbunden, da die Anlagen zunächst stillgelegt, gereinigt und im Anschluss von einer Behörde neu zertifiziert werden müssen. Somit verlängert sich die eigentliche Betriebsunterbrechungsdauer aufgrund von Reinigungsarbeiten durch die teilweise mehrere Monate dauernde Zertifizierung.

27.3.4 Technische und organisatorische Schutzmaßnahmen

Um die Ausmaße des Überschwemmungsrisikos zu begrenzen oder vorzubeugen, ist es wichtig, dass Vorsorgemaßnahmen getroffen werden. Allerdings wird immer ein Restrisiko bestehen, da selbst mit der besten Vorsorge nicht alle Schäden vermieden werden können. Die Schutzmaßnahmen, die ergriffen werden können, werden im Folgenden in technische und organisatorische Maßnahmen aufgeteilt.

27.3.4.1 Beispiele für technische Schutzmaßnahmen

Der erste Schritt, der Überschwemmungen vermeidet, ist, ein Gebäude außerhalb von Hochwasserzonen oder durch Aufschüttung ausreichend erhöht zu bauen. Bei bestehenden oder dennoch in Hochwasserzonen errichteten Gebäuden können Überschwemmungen durch den technischen Hochwasserschutz vorgebeugt werden. Es werden also zum Beispiel permanente Spundwände, Deiche oder Schutzmauern errichtet, um gefährdete Gebiete zu schützen. Diese Vorrichtungen müssen bereits vor dem Hochwasser vorhanden bzw. vorinstalliert sein, um im Schadenfall schnell einsatzbereit zu sein. Viele Städte oder Unternehmen stellen die Kosten und den Nutzen ins Verhältnis und greifen auf günstige Alternativen zurück, wie zum Beispiel Holzbalken oder Aluminiumbleche zum Aufstellen bzw. als Einschub.

Die technischen Maßnahmen können in permanente und temporäre Lösungen unterteilt werden. Zu den permanenten Lösungen zählen: eine erhöhte Bauweise, einzelne wichtige Anlagen, zum Beispiel Trafos erhöht zu bauen, IT und Elektrik aus dem Keller in erhöhte Bereiche zu verlagern, nicht unbedingt notwendige Türen, Tore und Kabel- bzw. Rohrtunnel zu verschließen oder stillzulegen, Einbau von Rückschlagklappen, Hochwasserwände einzuziehen (zum Beispiel um wichtige oder empfindliche Anlagen zu schützen). Temporäre Lösungen hingegen umfassen den Einbau von Hochwasserschutztüren, Verschlussystemen mit vorbereiteten Gleitschienen, das Umlagern von wichtigem oder wertvollem Lagergut, den Umbau und die Vorbereitung von Maschinen, damit sie rasch stillgelegt oder sogar in sichere Bereiche verlagert werden können. Dabei erfordern die temporären Lösungen einen Hochwassernotfallplan, welcher regelmäßig geübt und auf dem aktuellen Stand gehalten werden muss. Der Hochwassernotfallplan stellt eine organisatorische Schutzmaßnahme dar und wird im nächsten Kapitel genauer beschrieben.

Zur weiteren Begrenzung einer potenziellen Gefährdung dient die Reaktivierung von ursprünglichen, natürlichen Überschwemmungsgebieten. In Deutschland existiert mittlerweile nur noch ein Drittel der ehemaligen Überschwemmungsgebiete. Allerdings ist der Rückbau sehr aufwendig, da neben den baulichen Maßnahmen auch die Landwirte, denen die zukünftig im Überschwemmungsgebiet liegenden Flächen gehören, entschädigt werden oder Austauschzahlungen erhalten müssen. Eine weitere Möglichkeit bietet ein eingedeckter Uferbereich, der bei Bedarf geflutet werden kann und somit den Effekt einer Aue nachahmt. Am Rhein zum Beispiel sollen bis 2020 Überflutungsflächen von 1.000 Quadratkilometern geschaffen werden, damit der Pegel bei Hochwasser um bis zu 70 Zentimeter weniger stark ansteigt.

Seit 2005 besteht ein Gesetz in Deutschland, welches besagt, dass in gefährdeten Gebieten keine neuen Bau- und Gewerbegebiete mehr ausgewiesen werden dürfen. Genauso liegt es im Interesse von jedem Industriever sicherer, den Kunden von einem Neubau in einer Hochwasserzone abzuhalten. Bei bereits vorhandenen Bauten werden die Betroffenen aufgefordert, geeignete Vorsorgemaßnahmen zu treffen, um einen potenziellen Schaden zu vermindern. Um dies umzusetzen, sollte eine, an das Hochwasser angepasste, Bauweise gefördert werden. Hierunter zählt, wie zuvor aufgeführt, zum Beispiel das Auslassen von Kellern, eine höhere Bauweise oder das Anheben von kritischer Infrastruktur (vgl. Podbregar und Lohmann 2015, S. 202 ff.).

27.3.4.2 Beispiele für organisatorische Schutzmaßnahmen

Organisatorische Schutzmaßnahmen sind in der Regel einfacher bzw. kostengünstiger umzusetzen als technische. Ein Schwerpunkt bei organisatorischen Schutzmaßnahmen ist, dass diese für den Ernstfall geübt und die Verantwortungsbereiche klar zugeordnet werden müssen. Unternehmen, welche organisatorische Maßnahmen aktiv nutzen, haben signifikant weniger Schäden und zusätzlich geringere Schadendauern. Dies zeigt, dass Schutzmaßnahmen nicht immer teuer sind und auch schon kleinere Maßnahmen, welche gut organisiert sind, hohe Auswirkungen auf das Schadenausmaß haben können.

Um die Menschen und Sachwerte im Ernstfall zu schützen, bestehen Frühwarnsysteme. Bei dem Thema Hochwasser waren die USA Vorreiter, da sie viel in die Überwachung der Flüsse investiert haben und als Erste die Pegelstände der großen Flüsse mithilfe von Radar- und Satellitentechnik überwacht haben. Mittlerweile ist dies in den meisten Industrieländern üblich, so dass bei einem steigenden Wasserstand durch regelmäßige Pegelmessungen rechtzeitig vorgewarnt werden kann. Was rechtzeitig bedeutet, hängt allerdings von dem jeweiligen Unternehmen ab und welche Maßnahmen im Vorfeld getroffen werden müssen. Die Vorhersage für Hochwasser ist heutzutage viel genauer, als die von anderen Naturgefahren, wie zum Beispiel Bei Vulkanausbrüchen, da bereits die Messung der Pegelstände eine relativ genaue Vorhersage treffen kann. Frühwarnsysteme können größeren Schäden vorbeugen. Je nach Vorwarnzeit kann ein sehr kurzer oder auch ein langer Zeitraum eingeräumt werden, um geeignete Maßnahmen zur Schadenprävention treffen zu können. Bei kleinen Bächen oder Starkregen bleiben oft nur wenige Stunden, bis der Schaden eintritt.

Unter einem Hochwassernotfallplan sind organisatorische Maßnahmen zusammengefasst, welche kurz vor, während und nach einem Hochwasser eingreifen. Ein solcher Plan ist gerade bei Standorten mit einem hohen oder moderaten Risiko sinnvoll und wird häufig wie ein Handbuch niedergeschrieben. Hierbei ist eine Zusammenarbeit unter anderem auch mit den jeweiligen Behörden wichtig, da diese verschiedene Hochwasserwarnstufen haben und automatisierte Auskunft über die aktuelle Lage der Hochwasserwelle geben können. Ein hochwasserexponiertes Unternehmen muss das Szenario verstehen und wissen, woher es mögliche Hochwasserwarnungen erhalten kann. Neben den Behörden können gerade bei großen Flüssen auch Internetseiten oder Push-Nachrichten über ein kommendes Hochwasser informieren. Ab wann spezifische Maßnahmen ergriffen werden,

muss jedes Unternehmen für sich und in Zusammenarbeit mit seinen Sachversicherern definieren. Ein sinnvoller Parameter hierfür ist der Pegelstand des naheliegenden Flusses oder Baches. Das Unternehmen muss auf die lokalen Gegebenheiten achten, da die Auswirkungen regional sehr unterschiedlich sein können. So stand das Wasser beispielsweise im Sommer 2017 in Köln-Ehrenfeld nach einem Starkregen mehrere Zentimeter hoch, während es in Köln-Mülheim hingegen lediglich stark regnete, ohne dass sich das Wasser auf der Straße gesammelt hat. Die Zuständigkeiten für den Hochwassernotfallplan sollten hierarchisch im Management angesiedelt sein, damit im Ernstfall schnelle und rechtzeitige Entscheidungen getroffen werden können. Maßnahmen im Hochwassernotfallplan müssen konkret benannt und konkret beschrieben werden. Die zeitliche Reihenfolge der Maßnahmen muss festgelegt werden und es muss geklärt sein, wer die Tätigkeit ausführt und wie viel Zeit dies in Anspruch nimmt. Idealerweise wird der Hochwassernotfallplan einmal im Jahr geübt und es werden Stellvertreter für die entsprechenden Maßnahmen benannt.

Fest installierte Vorrichtungen für Schotts eignen sich meist besser, um Hochwasser abzuhalten als beispielsweise die Bevorratung von Sandsäcken. Schotts können in vergleichsweise kurzer Zeit geschlossen werden, während das Befüllen von Sandsäcken mehrere Personen sowie aufgrund der Zeitintensität eine längere Vorwarnzeit benötigt. Weiterhin ist es sinnvoll, Pumpen bereit zu halten, um zeitnah mit dem Abpumpen aus Gruben und Kellerräumen beginnen zu können.

Mit dem Eindringen von Wasser ist immer zu rechnen, auch wenn gute technische und organisatorische Maßnahmen bestehen. Im Hochwassernotfallplan muss also festgehalten werden, woher Pumpen beschafft werden können, falls nicht im Werk vorrätig, und dies sollte bestenfalls im Voraus vertraglich mit Anbietern vereinbart werden, sodass die Beschaffung zeitnah gesichert ist. Neben den Pumpen sind auch Trockengeräte frühzeitig zu beschaffen und erforderlich, um den Feuchtigkeitsgehalt schnell zu verringern.

Regelmäßig und nach jedem Schadenereignis bzw. Hochwasserevent muss der Hochwassernotfallplan angepasst werden. Hierzu wird reflektiert, was gut und was schlecht im Ablauf war und die Aktualität aller Informationen (Internetadressen, Aktualität der Firmen) muss geprüft werden. Das mögliche Schadenszenario muss hierbei sehr detailliert und bis zum Ende durchdacht sein. Bei einem hohen Schadenausmaß kann sogar in Betracht gezogen werden, den Standort zu verlagern, wenn der Ausfall einer Spezialmaschine im Schadenfall wahrscheinlich ist und daher eine sehr hohe Ausfallzeit und einen Stillstand der Produktion die Folge sein könnte.

Maßnahmen vor einem Hochwasser sind je nach Risiko beispielsweise das rechtzeitige Abschalten von Strom und Fertigungsanlagen, je nach Vorwarnzeit eine erhöhte Lagerung von Lagergut und Maschinen, das Imprägnieren von Produkten und Arbeitsmitteln (mit zum Beispiel Öl), um Korrosionsschäden zu verhindern. Während des Hochwassers ist vor allem der Personenschutz am wichtigsten. Außerdem sollte bereits zu diesem Zeitpunkt mit den Kunden und Lieferanten transparent kommuniziert werden und es sollte ein Informationsfluss für alle bestehen (zum Beispiel auch für die Mitarbeiter). Im Ernstfall wird auch bei Mitbewerbern angefragt, ob eine zeitweise (Teil-) Produktion übernommen

werden kann. Nach einem Hochwasser müssen Reinigungsfirmen, Aufräumarbeiten und Pumpen organisiert werden. Hierbei werden die eigenen Möglichkeiten oft überschätzt. So macht es zum Beispiel wenig Sinn, eine Pumpe bereits in Betrieb zu nehmen, wenn das Hochwasser noch steigt. Wenn Schlamm mit dem Wasser eingedrungen ist, sollte dieser schnell aus dem Gebäude entfernt werden, da Schlamm in trockener Form sehr hart wird und dann möglicherweise nur noch mit dem Presslufthammer beseitigt werden kann. Im Idealfall werden Schutzmaßnahmen dauerhaft installiert, so dass im Schadenfall der Hochwasserschutz bereits vorhanden ist, da organisatorische Maßnahmen stark auf den Faktor Mensch angewiesen sind.

Zusammenfassend ist zu erkennen, dass das Überschwemmungsrisiko eine häufig auftretende Naturgefahr ist, bei der es von Relevanz ist, vorsorglich einen Notfallplan auszuarbeiten und zu trainieren, damit die Schäden begrenzt werden.

27.3.5 Risikotransfer

Je nach Risiko können Versicherer verschiedene Versicherungssummen zeichnen. Hierzu muss zunächst geprüft werden, wo sich die Grenzen Brutto als auch Netto befinden. Brutto ist hierbei das Risiko vor Rückversicherung und Netto ist der Betrag nach Rückversicherung, also das, was von dem Erstversicherer getragen wird und nicht über die Rückversicherung gedeckt ist. Ab einer festgelegten Kapazität (abhängig vom einzelnen Versicherer) erfolgt der Risikotransfer an einen Rückversicherer. Viele Versicherer arbeiten mit einem Rückversicherer-Pool zusammen, sodass in der Regel keine neuen Rückversicherungspartner gesucht werden müssen und auf im Voraus vereinbarte Rahmenverträge zurückgegriffen werden kann. Diese werden jährlich erneuert. Sobald die Kapazitäten des Rückversicherer-Pools ausgeschöpft sind, kann zusätzliche Deckung über den fakultativen Rückversicherungsmarkt eingekauft werden. Eine Absicherung über den Kapitalmarkt ist ebenfalls möglich. Bei hochexponierten Standorten sind höhere Selbstbehälte üblich und es bestehen oft Limitierungen des Sublimits, um die Prämie in einem vertretbaren Rahmen zu halten. So können zum Beispiel nur zehn Millionen Euro versichert werden, obwohl das Risiko 17 Millionen Euro beträgt, sodass der Kunde bewusst unversichert ist und einen (sehr unwahrscheinlichen) Teil des Schadens selbst trägt. Der Selbstbehalt und die Limits dienen also als Stellschrauben für die Festlegung der Prämie und der Zeichnungskapazität. Der Kunde kann allerdings auch Schutzmaßnahmen vornehmen, um das Risiko zu minimieren. Diese Vorsorgemaßnahmen wirken sich ebenfalls auf die Prämie bzw. die Kapazitäten aus. Hierbei gilt: Je besser der Kunde Vorsorge betreibt, desto geringer wird das Risiko und somit auch die Prämie. Für den Versicherer bedeutet dies, dass er weniger oder keinen Rückversicherungsschutz einkaufen muss. Vorsorgemaßnahmen, die dem Kunden als eine Empfehlung vorgeschlagen werden, können als Kontrolle des Versicherers empfunden werden. In der Regel dauert es ein bis zwei Jahre, bis der Kunde verstanden hat, dass diese Vorsorgemaßnahmen vor allem in seinem Interesse sind, sodass diese Vorsorgemaßnahmen schneller umgesetzt werden.

Außerdem gibt es länderspezifische Besonderheiten, wie in Frankreich. Dort muss die Pflichtdeckung „Catastrophes Naturelles“ für bestimmte Naturkatastrophen, eingeschlossen werden. Das Risiko wird allerdings von einem Rückversicherer-Pool in Frankreich übernommen. Hierfür werden einheitlich zwölf Prozent der Nettoprämie an den Pool gezahlt, sodass Überschwemmungsrisiken in Frankreich nicht vom Versicherer des Kunden übernommen werden.

27.4 Risikomanagement von Naturgefahren

Um Naturgefahren besser einschätzen zu können, gibt es unterschiedliche Ansätze, die Risiken zu analysieren, zu steuern und zu bewerten. Diese Ansätze werden im Folgenden beschrieben.

Die allgemeine Risikobeurteilung kann quantitativ erfolgen, also durch die Schätzung der Eintrittswahrscheinlichkeit und Schadenhöhe, sodass das Risiko das Produkt der beiden Größen ist. Die Eintrittswahrscheinlichkeit und die Schadenhöhe sind allerdings nur mithilfe von stochastischen Modellen berechnet, wodurch eine gewisse Unsicherheit besteht und diese Werte nicht mit Sicherheit vorhergesagt werden können. Schätzungen beruhen in der Regel auf Vergangenheitswerten oder Statistiken. Bei vielen Naturgefahren ist diese Art von Beurteilung allerdings problematisch, da es nur wenige Vergangenheitswerte gibt (zum Beispiel bei sogenannten „Hundertjahresereignissen“, welche eine ungeheure Beschreibung der Eintrittswahrscheinlichkeit darstellen) und sich eine genaue Eintrittswahrscheinlichkeit somit nur sehr schwer berechnen lässt.

Eine weitere Möglichkeit bietet die qualitative Beurteilung, bei welcher das Risiko nach der Relevanz für das Unternehmen eingestuft wird. Diese Einstufung erfolgt durch Expertenschätzungen, ist daher allerdings auch subjektiv und hängt von der jeweiligen Risikowahrnehmung ab. Die Risikowahrnehmung ist normalerweise unternehmensspezifisch und wird durch die Unternehmens- und Risikokultur mitgestaltet. Weiterhin spielt es eine Rolle, welche Risikobereitschaft die Entscheidungsträger haben, zum Beispiel welche Risikobereitschaft im Unternehmen vorgegeben wird. Auch die öffentliche Wahrnehmung des Risikos sowie die Medienpräsenz beeinflussen die Einstufung des Risikos. So mit werden Ereignisse, bei denen viele Menschen betroffen sind, wie zum Beispiel ein Flugzeugabsturz oder ein Erdbeben, als gefährlicher eingestuft und auch als stärker wahrgenommen, als andere Ereignisse, bei denen nur wenige Menschen betroffen sind, wie zum Beispiel bei Lawinen. Auch der Zeitpunkt, zu dem das Ereignis letztmalig eingetreten ist, spielt im Hinblick auf die Risikowahrnehmung eine entscheidende Rolle, da Ereignissen, die weit zurück liegen, meist ein geringeres Risiko zugeordnet wird. Dies zeigt, dass die Risikobewertung bei solchen Ereignissen nur schwer vorzunehmen ist. Auch die Frage, ob das Risiko einer Naturgefahr vom Unternehmen getragen werden kann, ist nicht leicht zu beantworten. Daher sind Unternehmen in der Regel hiergegen versichert. Die Eintrittswahrscheinlichkeit kann relativ genau bestimmt werden, das Schadenausmaß kann allerdings sehr hoch sein, da komplette Gebäude zerstört werden können oder große

Betriebsunterbrechungsschäden entstehen, sodass eine Naturgefahrendeckung in den meisten Fällen sinnvoll ist. Die nächste Entscheidung, die das Unternehmen treffen muss, ist, wie die Risikosteuerung erfolgen soll. Soll eine Risikovermeidung, Risikoverminderung, ein Risikotransfer oder eine Selbsttragung erfolgen? Diese Fragen können nicht pauschal beantwortet werden, da die Antworten darauf stark von der Entscheidung des Unternehmens, den äußeren Einwirkungen sowie der Versicherbarkeit abhängen. Dabei sollte der Risikoumfang allerdings nicht größer als die Risikotragfähigkeit sein. Letztere ist ein Kern-element der Unternehmens- und Risikostrategie und beschreibt die Fähigkeit eines Unternehmens, mögliche Verluste aus identifizierten Risiken zu tragen, ohne dass daraus eine Gefahr für die Existenz des Unternehmens resultiert (vgl. Rohlfs 2018, S. 33 m. w. N.). Hierbei kann der Versicherungsschutz kleinerer Einheiten existenziell wichtig für diese sein, da zum Beispiel ein Totalschaden eines Gebäudes nicht allein von der Tochtergesellschaft getragen werden kann, vom Mutterkonzern allerdings schon. Im Einzelfall muss also entschieden werden, ob bestimmte Risiken eingegangen werden und welches Interesse überwiegt.

Mit der Risikotragfähigkeit besteht ein wichtiges Kriterium, welches bei der Entscheidung zur passenden Risikosteuerung eine Richtung weist. Zusätzlich zur Risikotragfähigkeit sollte auch das Chancen-Risiko-Verhältnis an die Umstände des Unternehmens angepasst werden und das Bruttonrisiko, soweit es geht, reduziert werden. Bei dem Bruttonrisiko handelt es sich um das ursprüngliche Risiko, welches vor den Steuerungsmaßnahmen besteht. Steuerungsmaßnahmen, um das Bruttonrisiko zu reduzieren, sind, wie zuvor erwähnt, die Risikovermeidung, die Risikoverminderung und der Risikotransfer. Das Restrisiko, welches nach den Maßnahmen übrig bleibt, wird vom Unternehmen selbst getragen. Bei der Risikovermeidung wird zum Beispiel das Risiko eines Erdbebens ausgeschlossen, indem erdbebengefährdete Gebiete komplett gemieden werden. Die Risikoverminderung ist ein Mittel, mit dem zum Beispiel die Anzahl der gefährdeten Standorte reduziert wird, indem nur eine begrenzte Anzahl an Kunden angenommen oder eine an die Naturgefahr angepasste Bauweise angewendet wird, sodass in gefährdeten Gebieten weiterhin Chancen auf einen Ertrag bestehen. Die letzte Steuerungsmaßnahme ist der Risikotransfer, bei dem das Risiko beispielsweise durch einen (Rück-)Versicherer getragen wird, damit hohe Risiken, die das Unternehmen nicht selbst steuern oder tragen kann, auch abgedeckt sind. Die Risikosteuerung von Naturgefahren ist in der Regel schwieriger als bei anderen Gefahren, da die Eintrittswahrscheinlichkeit sehr unwahrscheinlich und selten ist, das Schadensausmaß aufgrund des Kumulirisikos jedoch sehr hoch sein kann. Dies bedeutet, dass durch ein und dasselbe Ereignis gleichzeitig mehrere Schäden entstehen können. Daher scheidet eine komplette Selbsttragung seitens des Unternehmens in der Regel aus. Auch eine Vermeidung oder Verminderung des Risikos ist für die meisten Unternehmen nicht möglich, da bestimmte Standorte oder Tochtergesellschaften nicht verlegt werden können und sich in gefährdeten Gebieten befinden müssen, wie zum Beispiel Telekommunikationsunternehmen in den USA. Gerade in Großstädten wie San Francisco oder in Florida, wo sich viele Menschen befinden, müssen ausreichend viele Sendemasten vorhanden sein, damit das Mobilfunknetz auch dort funktioniert. Aber gerade in diesen Regionen ist das

Risiko für Stürme sehr hoch, sodass das Ausfallrisiko des Netzes nicht vermieden werden kann. Dafür können Maßnahmen wie zum Beispiel feste Generatoren oder die Errichtung von Plattformen ergriffen werden, um Schaltschränke vor Überschwemmungen zu schützen, sodass der Schaden so gering wie möglich ausfällt. Der Risikotransfer, also die Absicherung durch eine Versicherung, ist in gefährdeten Gebieten daher zusätzlich empfehlenswert. Aber gerade die Versicherbarkeit von Naturgefahren ist in der Regel stark begrenzt oder sehr teuer, da es sich bei Naturgefahren fast immer um ein Kumulrisiko handelt. Es werden in der Regel hohe Selbstbehalte vereinbart, damit das Risiko im Schadenfall nicht ausschließlich vom Versicherer getragen werden muss. Das Prinzip einer Versicherung funktioniert, da ein Ausgleich im Kollektiv stattfindet und eine große Anzahl an Risiken im Portfolio des Versicherers vorhanden ist. Dadurch findet das Gesetz der großen Zahlen in diesem Bereich Anwendung. Dieses besagt folgendes: Je größer die Anzahl der Risiken mit der gleichen Gefahr ist, desto geringer wirken sich Schwankungen auf den Erwartungswert aus, sodass der Ausgleich im Kollektiv bei einem ausreichend großen Bestand funktioniert und der Versicherer somit selbst große Einzelschäden durch die weiteren Risiken ausgleichen kann.

Hierbei ist es wichtig, dass der Versicherer seine Risiken diversifiziert, also die Einzelrisiken streut und diese nicht positiv miteinander korrelieren. Da Naturgefahren großflächige Schäden verursachen, findet das Gesetz der großen Zahlen nur bedingt Anwendung. Daher ist es umso wichtiger, dass das Portfolio des Versicherers unterschiedliche Risiken aufweist, sodass Großschäden durch Naturgefahren auch spartenübergreifend ausgeglichen werden können. Sofern in einem Jahr dennoch sehr hohe Schäden entstanden sind, können diese auch mithilfe der Schwankungsrückstellung über die nächsten Jahre ausgeglichen werden. Bei Naturgefahren ist dies häufig der Fall, da sie seltener auftreten als klassische Versicherungsschäden wie zum Beispiel Unfälle oder Diebstahl (Frequenzschäden). Im Schadenfall ist es wichtig, gut vorbereitet zu sein. Zum einen kann der Schaden durch Frühwarnsysteme bereits im Voraus begrenzt werden, und zum anderen ist das Krisenmanagement der Kunden und auch des Versicherers enorm wichtig, um schnelle Hilfe leisten zu können. Hierbei werden unter anderem knappe Ressourcen, wie zum Beispiel Handwerker oder Lebensmittel, bereits im Voraus organisiert, das Personal wird in der betroffenen Region verstärkt und ein Netzwerk von Handwerkern und Dienstleistern wird aktiviert, sodass die Schäden bestmöglich beseitigt werden können.

Es sollte weiterhin ein Business Continuity Management (BCM) bestehen, also Strategien und Pläne, welche im Falle einer Betriebsunterbrechung den Geschäftsbetrieb aufrechterhalten. Durch die Globalisierung und die zunehmende Vernetzung der Wirtschaft, des Handels und der Industrie kann eine Naturgefahr, von der ein Unternehmen nicht direkt betroffen ist, dennoch enorme Auswirkungen haben, da Zulieferer oder auch Abnehmer betroffen sein können. Somit ist neben der Reputation auch die Existenz bedroht. So war es auch bei der Nuklearkatastrophe von Fukushima im Jahr 2011. Dort wurde ein Werk des Chemie- und Pharmaunternehmens Merck aufgrund des Erdbebens geschlossen. Dieses Werk stellte als einziges ein Pigment her, welches in vielen Metallic-Lackierungen für Kraftfahrzeuge verwendet wird, sodass es weltweit zu Lieferproblemen bei einer

Vielzahl von Autobauern kam, welche mit dem Pigment Spezialfarben herstellen. Ein BCM analysiert zunächst, welche Geschäftsprozesse unabdingbar sind, und prüft im nächsten Schritt, wie anfällig diese Geschäftsprozesse für Risiken sind. Daraufhin wird ein Geschäftsfortführungsplan für den Ernstfall erstellt. Dieser ganze Prozess sollte regelmäßig geprüft und verbessert und schriftlich festgehalten werden, sodass der Prozess im Schadenfall einwandfrei läuft (vgl. GDV 2017, S. 24 f.).

27.5 Ausblick: Naturgefahren in der Zukunft

Die grundsätzliche Einschätzung von Naturgefahren seitens der Versicherer hat sich nicht geändert, da sich das bisherige Vorgehen mithilfe von Modellierungen im Allgemeinen bewährt hat. Hierbei werden mögliche Schadenverläufe und somit eine Schätzung der Schadenerwartungen und Schadenausmaße von Großrisiken modelliert. Das Modell der Versicherer wird regelmäßig aktualisiert und an neue oder veränderte Gefahren angepasst, sodass es auf dem neuesten Stand ist und die Erfahrungen aus vorherigen Schadenereignissen in der nächsten Modellierung berücksichtigt werden können. Auch andere Faktoren, wie zum Beispiel der Klimawandel, der im Allgemeinen die Eintrittswahrscheinlichkeit von Naturgefahren erhöht, werden mithilfe einer stärkeren Gewichtung dieser Eintrittswahrscheinlichkeit berücksichtigt.

Bereits heute wird bei Dämmen und Deichen in Küstennähe in vielen Fällen ein Klimazuschlag berücksichtigt, sodass die Dämme höher gebaut werden, um dem steigenden Meeresspiegel in der Zukunft entgegenzuwirken. Aus Unternehmenssicht haben Naturgefahren im Jahre 2020 im Vergleich zum Jahre 2019 an Bedeutung verloren, da vor allem Cyberrisiken und auch Politische Risiken stärker in den Fokus getreten sind, wie es aus dem „Allianz Risk Barometer 2020“ zu erkennen ist. Dennoch befinden sich Naturgefahren auf Platz 4 der Top-Risiken. Aber auch das Risiko „Klimawandel/steigende Volatilität des Wetters“, welches im engen Zusammenhang mit Naturgefahren und deren häufigerem Auftreten steht, taucht im Jahr 2018 auf der Übersicht der zehn wichtigsten globalen Geschäftsrisiken erstmals auf (vgl. Allianz 2019) und befindet sich im Jahr 2020 bereits auf Platz 7. Im Rahmen des Risk Barometers werden Kunden des Versicherungskonzerns Allianz und Versicherungsmakler zu ihrer Einschätzung unterschiedlicher Risiken befragt. In dem Bericht aus dem Jahr 2020 haben insgesamt 2.718 Personen aus 102 Ländern teilgenommen, was aktuell die höchste Teilnehmerzahl des jährlichen Allianz Risk Barometers darstellt (vgl. Allianz 2020). Die versicherten Schäden, die im Jahre 2019 durch Naturkatastrophen ausgelöst wurden, haben im Vergleich zu den Vorjahren abgenommen. Dennoch waren die Waldbrände in Australien und Taifune in Asien häufig in den Schlagzeilen, was die Wichtigkeit dieses Risikos für Unternehmen erklärt. Diese befürchten, dass auch im Zusammenhang mit dem Klimawandel eine steigende Häufigkeit und eine wachsende Intensität der Naturgefahren bestehen, sodass eine Sensibilisierung für diese Gefahr erfolgt ist.

Wetterextreme wie Hitzewellen, Starkregen, Überschwemmungen und starke Dürreperioden haben seit den letzten Jahrzehnten zugenommen. Dies lässt sich zum großen Teil auf den Klimawandel zurückführen (vgl. Heep-Altiner und Berg 2014, S. 31).

Aus Unternehmenssicht haben Naturgefahren aufgrund der zunehmenden Häufigkeit eine höhere Bedeutung und sind weiter in den Fokus gerückt als zuvor. Aufgrund von Werteverdichtung und globalen Lieferabhängigkeiten können sich die gesamtwirtschaftlichen Auswirkungen von Naturgefahren wahrscheinlich erheblich verstärken.

Die wachsende Bevölkerung, Besiedlung von exponierten Gebieten, globale Vernetzung von Lieferketten, Wertekonzentrationen etc. sind nur einige Beispiele, welche zu einer wachsenden Betroffenheit von Naturgefahren sowie resultierenden Schäden führen.

Auch in Zukunft werden die Quantifizierung von Schäden und ihr zeitliches und örtliches Eintreten schwer zu bemessen sein. Die Auswirkungen der Naturgefahren werden mit einer hohen Wahrscheinlichkeit vom Klimawandel verstärkt, da sich daraus Änderungen in den unterschiedlichen Wetterphänomenen ergeben. Dadurch werden sich die zufällig auftretenden Naturgefahren in der Zukunft verändern (vgl. Heep-Altiner und Berg 2014, S. 39).

Literatur

- Allianz. (2019). Die größten Geschäftsrisiken für 2018. *Allianz Risk Barometer 2018*.
- Allianz. (2020). *Allianz Risk Barometer, Identifying the Major Business Risks for 2020*.
- Dikau, R., & Voss, H. (2000). *Naturkatastrophe*. Heidelberg: Spektrum Akademischer. <https://www.spektrum.de/lexikon/geowissenschaften/naturkatastrophe/10985>. Zugegriffen am 31.08.2020.
- GDV. (2017). *Naturgefahrenreport 2017*. <https://www.gdv.de/resource/blob/11662/d69427a10ce7f276ff35b21901f9648c/publikation%2D%2D-naturgefahrenreport-2017-data.pdf>. Zugegriffen am 31.08.2020.
- Heep-Altiner, M., & Berg, M. (2014). *Katastrophenmodellierung – Naturkatastrophen, Man Made Risiken, Epidemien und mehr* (Bd. 6, F. a. Köln, Hrsg.). Köln, Nordrhein-Westfalen, Deutschland. https://cos.bibl.th-koeln.de/frontdoor/deliver/index/docId/51/file/6_2014.pdf.
- Munich Re. (2018). Topics Geo Naturkatastrophen 2017, Ein Jahr der Stürme. https://www.munichre.com/content/dam/munichre/global/content-pieces/documents/302-09091_de.pdf. Zugegriffen am 31.08.2020.
- Podbregar, N., & Lohmann, D. (2015). *Im Fokus: Naturkatastrophen, Zerstörerische Gewalten und tickende Zeitbomben*. Berlin/Heidelberg: Springer.
- Rohlf, T. (2018). *Risikomanagement im Versicherungswesen – Identifizierung, Bewertung und Steuerung*. Karlsruhe: Versicherungswirtschaft.

Malwine Tewes ist bei FM Insurance Europe S. A. als Account Engineer tätig und beschäftigt sich seit vielen Jahren mit den Aspekten der Risikoanalyse, -identifizierung und damit einhergehender Risikoverbesserung durch entsprechende Maßnahmen in der Schadensprävention. Nach ihrem Bauingenieurstudium fand sie den Weg in die Industriever sicherung, wo sie seit 2003 als beratende Ingenieurin auf Kunden- sowie Versicherungsseite arbeitet.

Andrea Scholtes (ehemals Kittner) studierte Versicherungswesen mit den Schwerpunkten Risikomanagement, HUKR und Versicherungsmathematik am Institut für Versicherungswesen der Technischen Hochschule Köln. Im Anschluss absolvierte sie dort auch das Masterstudium Risk & Insurance. Während des Bachelorstudiums studierte sie ein Semester an der University of Limerick in Irland. Seit Studienbeginn arbeitet sie bei der Deutschen Telekom Assekuranz, bei der sie heute in dem Bereich industrielle Sachversicherungen tätig ist.



Transport und Warenkredit

28

Umgang mit spezifischen Risiken bei Handelsgeschäften

Reiner Siebert und Lukas Spohr

Zusammenfassung

Dieser Beitrag stellt Methoden für den Umgang mit Risiken des Warenhandels vor. Im Anschluss an die Erfassung und Analyse der Risikolandschaft von Handelsgeschäften wird der Leser über wesentliche Aspekte der Gütertransport- und der Warenkreditversicherung informiert, denn am Ende der Kette von Riskmanagement-Maßnahmen stellt sich die Frage nach Art und Umfang eines möglichen Risikotransfers auf Versicherungsgesellschaften. Im Fokus der Betrachtungen steht der Wertbeitrag, den Versicherungen im Rahmen des Risikomanagements für Unternehmen leisten können. Der letzte Abschnitt behandelt die Vermeidung bzw. Minderung von Forderungsausfall- und Transportschäden und schließt mit Handlungsempfehlungen ab.

28.1 Einführung

Dieses Kapitel befasst sich mit der Frage, inwieweit sich Risiken des Warenhandels kontrollieren lassen. Die Risikofaktoren sind unterschiedlicher Natur. Von der Vermeidung über die Minderung bis hin zur Übertragung der Risiken werden sowohl Aspekte möglicher Versicherungslösungen als auch Maßnahmen zur Schadenprävention erörtert.

R. Siebert

Gesamtverband der versicherungsnehmenden Wirtschaft e. V., Bonn, Deutschland

E-Mail: reiner.siebert@gvw.de

L. Spohr (✉)

TH Köln, Institut für Versicherungswesen, Köln, Deutschland

E-Mail: Lukasspohr@gmail.com

Durch eine Kreditversicherung werden Kaufverträge aus Sicht des Lieferanten gegen einen Ausfall der vereinbarten Forderung abgesichert. Ist der Kaufvertrag zustande gekommen und werden Waren versandt, sind es diverse Risiken, durch die die Güter beschädigt oder zerstört werden oder abhandenkommen können. Ist ein Schadenfall eingetreten, spielt die Gefahrentragung für beide Kaufvertragspartner eine übergeordnete Rolle. Sie wird deswegen anhand einiger vertraglicher Ausgestaltungsmerkmale näher beleuchtet.

Die Transportversicherung bietet im Rahmen einer Allgefahrendekoration umfangreichen Versicherungsschutz für die Beförderung und die Zwischenlagerung von Gütern. Der Regeldeckungsumfang kann durch Klauseln und Individualvereinbarungen dem jeweiligen Bedarf angepasst werden.

Nachstehend werden Anhaltspunkte und Anregungen für die Gestaltung eines sinnvollen Umgangs mit den Risiken des Warenhandels vorgestellt.

28.2 Risikoanalyse

Zentrales Thema dieses Abschnitts ist die Risikoanalyse von Handelsgeschäften und des Transports von Gütern.

28.2.1 Risikobeschreibung und Ursachen

Wer Handelsgeschäfte betreibt, wird mit Risiken dieser Geschäfte konfrontiert. Strukturiert betrachtet kann man die Risiken aus Handelsgeschäften von denen aus der Beförderung und Lagerung des gehandelten Gutes abgrenzen.

Das Handelsgeschäft birgt insbesondere Kreditrisiken. Hierbei sind in erster Linie der vollständige Forderungsausfall und der teilweise Forderungsausfall zu nennen. Diese Risiken sind versicherbar und können weitgehend im Rahmen einer Warenkreditversicherung aufgefangen werden.

Beim Abschluss der Kreditversicherung überträgt der Versicherungsnehmer das Risiko des Forderungsausfalls auf den Kreditversicherer, der im Schadenfall leistet. Im Falle eines Insolvenzverfahrens oder dem Vorliegen des Nichtzahlungstatbestandes (sogenanntes protracted default) kann indessen der vom Kreditversicherer beauftragte Dienstleister im Forderungsmanagement die Geschäftsbeziehung zwischen dem Versicherungsnehmer und dessen Vertragspartner erheblich belasten. Insbesondere Irrtümer können sich hier negativ auf das Verhältnis des Versicherungsnehmers zu seiner Kundschaft auswirken (vgl. Gerling Konzern 1985, S. 103).

Darüber hinaus können Zahlungen in Verzug geraten. Solche Fristüberschreitungen sind regelmäßig dem Versicherer anzusehen. Geschieht dies nicht rechtzeitig, besteht die Gefahr, dass ein Versicherer bei einem finanziell schwächeren Kunden keine Auffälligkeit erkennt, bevor ein Zahlungsausfall eintritt. Die Hereinnahme von Wechseln erhöht das

Risiko des Zahlungsverzugs und ist dem Kreditversicherer gegenüber ebenfalls grundsätzlich anzugepflichtig. Dies sollte bei der Auswahl der Zahlungsmodalitäten berücksichtigt werden (vgl. Gerling Konzern 1985, S. 104 ff.). Die Funktionalität des Versicherungsschutzes wird später dargelegt.

Die Beförderung und Zwischenlagerung von Handelsgütern bietet ein großes Spektrum an Risikoquellen. Ausgehend von der Wahl des Transportgutes, der Transportmittel (zum Beispiel See-/Binnenschiffe, Flugzeuge, Schienenfahrzeuge oder Lastkraftwagen), der Verpackung (zum Beispiel Container, Paletten, Kisten oder Paket) und der Sicherung der Transportgüter, entstehen durch statische und dynamische Belastungen, denen die Güter mit ihrer Verpackung ausgesetzt sind, physikalische und klimatische Risiken. Dies können einerseits Risiken sein, deren Realisierung die Beschädigung oder die Zerstörung des Gutes zur Folge haben. Andererseits kann ein Gut durch klimatische Veränderung oder infolge einer unzureichenden Verpackung Schaden nehmen.

Ferner ist der Verlust durch Diebstahl oder das Abhandenkommen in der Obhut eines Verkehrsdienstleisters ebenso denkbar wie kaufmännische (Haftungs-)Risiken, die durch die Wahl der Lieferbedingung entstehen. Stationäre Risiken der Lagerung oder der Zwischenlagerung sind ebenso nicht außer Acht zu lassen (vgl. Suhr 2017, S. 10). Um die Vielfalt an Risiken aufzufangen, bieten die einschlägigen Bedingungskonditionen zur Warentransportversicherung (DTV-Gütersicherungsbedingungen) zwei Deckungsformen an: die „volle Deckung“ im Sinne einer Allgefahrenversicherung und die „eingeschränkte Deckung“ mit einem abschließenden Katalog an benannten versicherten Gefahren. Letztgenannte Deckungsform soll insbesondere das Großschaden- und Katastrophenrisiko abdecken (vgl. Gerling 2007, S. 279).

28.2.2 Versicherbarkeit von Risiken des Warenhandels

Die Schadenversicherung definiert den Gefahrbegriff als die Möglichkeit nachteiliger Ereignisse, die eine ausreichende Unwägbarkeit bezüglich des Schadeneintritts und seines Zeitpunktes haben muss. Die Gefahr bedroht ein Interesse und kann ursächlich für einen Schaden sein. Diese Bedingungen müssen grundsätzlich erfüllt sein, um ein Risiko versicherbar zu machen (vgl. Ehlers 2001, S. 50).

Klassischerweise werden solche Gefahren nicht versichert, die aufgrund ihrer Häufigkeit nahezu vorhersehbar sind oder in ihrem Ausmaß nicht kalkuliert werden können. Wie der Reaktorunfall in Tschernobyl oder der Terrorakt des 11. September 2001 zeigen, ist nicht absehbar, welche Folgen solche Ereignisse nach sich ziehen können (vgl. Ehlers 2001, S. 101).

Die Rechtsgrundlagen der Warentransportversicherung sind zunächst das BGB und das VVG. Das Gesetz über den Versicherungsvertrag erklärt sich indessen nach § 209 VVG für grundsätzlich nicht zuständig, unter Ausnahme der reinen Binnentransportversicherung. Hier bildet das VVG (Kapitel 3, Transportversicherung, §§ 130 bis 141 VVG) zwar die Rechtsgrundlage, allerdings dürften die meisten Versicherungsverträge für Binnentransporte auf Basis von Seever sicherungsbedingungen abgeschlossen werden. Die Verträge

basieren deswegen im Wesentlichen auf Allgemeinen Versicherungsbedingungen, Klauseln sowie Sonderbedingungen. In Anwendung befinden sich aktuell die Allgemeinen Deutschen Seeverversicherungsbedingungen (ADS Güter 73/84), die DTV-Gütersicherungsbedingungen (DTV-Güter) sowie die Institute Cargo Clauses (ICC). Die ICC sind die englischen Versicherungsbedingungen für Warentransporte. Klauseln des ICC sind international anerkannt und können auch in Verträge auf Basis der ADS oder der DTV-Gütersicherungsbedingungen einbezogen werden (vgl. Gerling 2007, S. 276).

Im Folgenden wird lediglich auf die DTV-Güter näher eingegangen, um die Ausgestaltung des Versicherungsschutzes zu skizzieren, da diese im deutschen Markt eine bedeutende Rolle einnehmen.

28.2.3 Schadenbeispiel

Ist ein Güterkauf nach den Incoterms 2020, Klausel FCA-Bestimmungsort, zur Lieferung „Frei Frachtführer“ vereinbart und das Gut wird vor Übergabe an den Frachtführer beschädigt oder geht verloren, so ist dem Käufer des Gutes noch kein versicherbares Interesse entstanden. Er ist nicht zur Zahlung des Kaufpreises verpflichtet. Wird die Ware jedoch auf dem Haupttransportweg beschädigt, so erleidet der Käufer den wirtschaftlichen Schaden, denn er muss trotz des Schadens den Kaufpreis an den Verkäufer entrichten.

28.3 Umgang mit Transport- und Warenkreditversicherungsrisiken

28.3.1 Warentransportversicherung

Grundsätzlich besteht für die Handelsparteien keine Versicherungspflicht für Transporte. Jedoch ist die Warentransportversicherung für die Verkehrs- und Handelsindustrie unentbehrlich geworden, da durch sie das Risiko gegen Zahlung einer Prämie kalkulierbar geworden ist. Sie unterstützt somit die Handelsausweitung und den weltweiten Ex- und Import.

Die Relevanz der Warentransportversicherung wird auch bei Transporten ersichtlich, die von mehreren Verkehrsdiestleistern organisiert und durchgeführt werden. Im Falle einer Beschädigung des Transportgutes wird die Beweisführung, unter wessen Obhut sich das Gut zum Zeitpunkt der Beschädigung befand, erschwert und ist mitunter nicht mehr möglich. Hier hilft der Transportversicherer aus, indem er die Regressnahme übernimmt.

Als Ausnahme von der Regel ist beim internationalen Transport unter Einbeziehung der Incoterms-Klauseln CIF-Bestimmungsort („Cost, Insurance and Freight“, „Kosten, Versicherung und Fracht“) und CIP-Bestimmungsort („Carriage and Insurance Paid to“, „Fracht frei versichert“) die Transportversicherung verpflichtend vom Verkäufer zu besorgen. Auch Außenhandelsgeschäfte auf Grund eines Akkreditivs verlangen häufig die Absicherung des Transports (vgl. Gerling 2007, S. 274 f.).

28.3.1.1 Versicherungsfall/Definition

In den vom Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GDV) zur Anwendung in Versicherungsverträgen empfohlenen DTV-Gütersicherungsbedingungen (DTV-Güter 2000/2011) werden die versicherten Gefahren und Schäden im Rahmen der „vollen Deckung“ wie folgt behandelt:

„Der Versicherer trägt alle Gefahren, denen Güter während der Versicherung ausgesetzt sind, sofern nichts anderes bestimmt ist.“

„Der Versicherer leistet ohne Franchise Ersatz für Verlust oder Beschädigung der versicherten Güter als Folge einer versicherten Gefahr.“

Damit wird eine sogenannte Allgefahrendockung verankert. Das heißt, dass der Versicherer grundsätzlich alle Gefahren trägt, soweit die DTV-Güter 2000/2011 oder individuelle Vereinbarungen im Versicherungsvertrag nichts anderes bestimmen. Hierzu gibt es einen Katalog mit benannten Gefahren, die aus dem Versicherungsschutz ausgeschlossen sind. Außerdem wird der Versicherungsschutz durch Schadenausschlüsse begrenzt. Einzelne Tatbestände ausgeschlossener Gefahren können im Rahmen weitestgehend standardisierter Klauseln wieder in den Deckungsumfang eingeschlossen werden.

Die „eingeschränkte Deckung“ hingegen bezieht sich auf eine Liste benannter Gefahren, für die Versicherungsschutz besteht.

*„Der Versicherer leistet ohne Franchise Ersatz für Verlust oder Beschädigung der versicherten Güter als Folge der **nachstehenden Ereignisse**.“*

Folgende Gefahren sind versichert: Unfall des Transportmittels, Brand, Blitzschlag, Explosion, Erdbeben, Seeboden, vulkanische Ausbrüche und sonstige Naturkatastrophen, Anprall oder Absturz eines Flugkörpers, seiner Teile oder seiner Ladung.

Darüber hinaus sind Überbordwerfen, Überbordspülen oder Überbordgehen durch schweres Wetter, Aufopferung der Güter, Gefahren des Umschlags an Nothäfen, die aufgrund einer versicherten Gefahr angesteuert werden, und Totalverlust ganzer Kolli beim Be-, Um- oder Entladen eines Transportmittels versichert. Diese Ereignisse werden im Folgenden kurz erläutert.

Überbordgehen durch schweres Wetter meint den Verlust auf Deck geladener Güter, zum Beispiel durch mangelhafte Befestigung bei schwerer See. Häufig ist unzureichendes Lasching (siehe späteres Kapitel) in Verbindung mit hohen Bewegungskräften Ursache für den Verlust der Ware.

Werden Transportgüter aufgegeben, um Schlimmeres zu verhindern, spricht man von Aufopferung im Sinne der Bedingungen. Typischerweise fallen hierunter Maßnahmen, wie zum Beispiel Ballastabwerfen oder Fluten des Ladungsraumes, um das Schiff bzw. das Transportmittel zu schützen.

Die Nothafenklause deckt das versicherte Gut im Rahmen einer Allgefahrendockung für den Zeitraum ab, in dem Güter im angesteuerten Nothafen (Flug- und Schiffshafen) verladen und zwischengelagert werden.

Der Totalverlust ganzer Kolli bezeichnet den wirtschaftlichen Totalschaden einer Ladungseinheit. Dabei kann einerseits die Substanzvernichtung der Beschädigung beim Verladen oder der Besitzverlust (zum Beispiel Paket fällt ins Wasser) gemeint sein. Ein Kollo definiert eine selbstständige Einheit eines Ladungsstücks, nicht die Gesamtheit der zu verladenden Güter (vgl. Gerling 2007, S. 274 ff.).

28.3.1.2 Marktübliche Bedingungen und Klauseln in der Warentransportversicherung

Wie bereits dargestellt, gibt es mehrere marktübliche Bedingungswerke. Deren Deckungs- umfang wird durch die DTV-Güter 2000/2011 weitgehend abgebildet, deswegen nehmen die folgenden Ausführungen Bezug auf diese Bedingungskonditionen.

Nach Ziff. 1.1 der DTV Güter 2000/2011 können sämtliche wirtschaftlichen, in Geld schätzbaren Interessen an der schadenfreien Beförderung oder Lagerung eines Transportgutes während der Dauer der Versicherung versichert werden. Explizit sind Güter oder Güterarten der im Vertrag bestimmten Art versichert und/oder sonstige Aufwendungen bzw. Kosten. Die Formulierung „und/oder“ soll verdeutlichen, dass losgelöst von Güterschäden auch oder separat Aufwendungen bzw. Kosten Gegenstand des Versicherungsvertrages werden können. Beispiele für diese Position sind der folgenden Aufzählung zu entnehmen:

- Beitrag zur großen Haverei,
- Schadenabwendungs-, Schadenminderungs-, Schadenfeststellungskosten,
- Kosten der Ermittlung oder Feststellung des versicherten Schadens.

Zusätzlich können folgende Interessen mitversichert werden:

- Interesse des imaginären Gewinns; der imaginäre Gewinn entspricht dem vom Empfänger des Gutes erwartete Gewinn bei Eintreffen der versicherten Sache am Bestimmungsort.
- Interesse des Mehrwerts; der Mehrwert berücksichtigt beispielsweise Wertsteigerungen zwischen Abschluss des Versicherungsvertrages und Transportzeitpunkt und beugt somit einer Unterversicherung vor. Die Mitversicherung von Mehrwert hat eine hohe praktische Bedeutung, wie Preisschwankungen bei Verbrauchsgütern wie Kaffee oder Kakao zeigen (vgl. Ehlers 2001, S. 41).
- Sonstige Aufwendungen und Kosten; hierunter fallen beispielsweise Zoll, Fracht, Steuern und Abgaben, soweit diese nicht bereits im Fakturawert enthalten sind.
- Interesse von Dritten; das Interesse eines Dritten kann im Sinne der Versicherung für fremde Rechnung abgesichert werden. Diese Regelung ist insbesondere bei den Incoterms 2020-Klauseln CIF- und CIP-Bestimmungsort wichtig, da hier der Versicherungsnehmer in seiner Eigenschaft als Exporteur vertraglich angehalten ist, die Versicherung für fremde Rechnung abzuschließen. Wer der Interessenträger ist, kann bei Abschluss des Versicherungsvertrages zunächst offenbleiben. Die Transportversiche-

rung kann „für Rechnung, wen es angeht“ genommen werden. Spätestens im Schadefall ist jedoch das versicherte Interesse nachzuweisen, dann muss auch der Inhaber des Interesses feststehen.

Nicht versichert oder gesondert einzuschließen sind im Wesentlichen Gefahren, die aus politischen oder sozialen Auseinandersetzungen, wie Krieg, Bürgerkrieg, Streik, Aussperung, Arbeitsunruhen, sowie Sanktionen, Beschlagnahme, Entziehung oder sonstiger Eingriffe der hohen Hand, erwachsen (sogenannte politische Gefahren). Auch die Risiken der Zahlungsunfähigkeit oder der sonstigen finanziellen Auseinandersetzungen mit einem ausführenden Verkehrsträger sind vorerst nicht versichert. Anfang des Jahres 2004 sind die Ausschlüsse von den Gefahren ionisierender Strahlungen oder von chemischen, biologischen, biochemischen Substanzen oder elektronischen Wellen als Waffe, der sogenannte Dirty-Bombs-Schadenausschluss, hinzugekommen.

Neben den Gefahrenausschlüssen gibt es einige Schadenausschlüsse, wie die Verzögerung der Reise, innerer Verderb, handelsübliche Mengen-, Maß- oder Gewichtsdifferenzen, gewöhnliche Temperaturschwankungen oder mittelbare Schäden aller Art (vgl. Ehlers 2001, S. 50 ff.).

Beim Ausschluss für Schäden durch eine unzureichende Verpackung der Ware gehen die ADS-Güter 73/84 und DTV-Güter 2000/2011 unterschiedliche Wege, mit weitreichenden Folgen. Nach den ADS Güter 73/84 leistet der Versicherer keinen Ersatz für das Fehlen oder Mängel „handelsüblicher“ Verpackung. Ist eine Ware handelsüblich verpackt, ist ein Schaden im Sinne der Versicherungsbedingungen selbst dann grundsätzlich versichert, wenn die Verpackung objektiv mangelhaft war. Die DTV-Güter 2000/2011 beziehen sich in diesem Zusammenhang demgegenüber auf eine „beanspruchungsgerechte“ Verpackung, mit Entlastungsmöglichkeit für ein fehlendes qualifiziertes Verschulden. Die beanspruchungsgerechte Verpackung definiert der GDV als den tatsächlich vorliegenden Gegebenheiten der geplanten Reise entsprechend verpackt. Diese Anforderung zu erfüllen, ist so gut wie unmöglich, weil die Güterverpackung auch Belastungen eines ungewöhnlichen Reiseverlaufs standhalten muss (vgl. Tittko 2015, S. 20 ff.). Hat der Versicherte einen Dritten mit der Verpackung beauftragt, so muss er sich dessen Verhalten zurechnen lassen. Die wesentlichen Aspekte der Verpackungsqualität werden später thematisiert.

28.3.1.3 Versichertes Interesse und Deckungsformen der Warentransportversicherung

In Handelsgeschäften haben die Parteien eines Kaufvertrages ein „Interesse“ an der Erfüllung des Geschäfts. Es soll vermieden werden, *wirtschaftlichen* Schaden aus dem Geschäft zu erleiden. Wie im vorherigen Abschnitt dargestellt, können bei dem Transport von Gütern unterschiedliche Interessen entstehen, um sich gegen Schadeneignisse abzusichern.

Dieses versicherbare Interesse orientiert sich im Wesentlichen an der Gefahrtragung für Verlust oder Beschädigung des Transportgutes. Die im Kaufvertrag vereinbarten Lieferbedingungen regeln die Gefahrtragung. So setzen die sogenannten Incoterms (kurz für: International Commercial Terms der Internationalen Handelskammer, Paris) per Klausel fest,

wo und zu welchem Zeitpunkt Gefahren und Kosten vom Verkäufer auf den Käufer übergehen. Besonders ist hier, dass mehrere Parteien ein versicherbares Interesse an derselben Sache haben (vgl. Gerling 2007, S. 130).

28.3.2 Warenkreditversicherung

Die indirekte Liquiditätsversorgung durch Lieferantenkredite ist im Laufe der Globalisierung des Handels größer geworden als die direkte Liquiditätsversorgung durch Betriebsmittelkredite.

Die nicht selten schwache Eigenkapitalausstattung der Unternehmen in Deutschland erhöht den Druck auf die Liquidität. Die flüssigen Mittel der Unternehmen stammen neben den Betriebsmittelkrediten zu großen Teilen aus Lieferantenkrediten. Fällt die Zahlung eines Lieferantenkredites, also die Forderung aus Lieferung und Leistung, aus, kann dies zu einem Liquiditätsengpass führen. Es entsteht mithin ein Sicherungsinteresse des Lieferanten, bezogen auf dessen Forderungen. Diesem Interesse entgegengerichtet werden Lieferantenkredite in den meisten Fällen gewährt, um keine Wettbewerbsnachteile zu erleiden. Um den Zahlungsausfall seines Kunden zu vermeiden oder abzusichern, stehen dem Lieferanten viele Möglichkeiten zur Verfügung (vgl. Gerling 2007, S. 80) (Tab. 28.1).

28.3.2.1 Versicherungsfall/Definition

Der Forderungsausfall, der aufgrund einer Insolvenz des Kunden entsteht, wird vom Versicherer nach Maßgabe der einschlägigen Bedingungsstandards ersetzt. Als Versicherungsfälle gelten:

- das eröffnete Insolvenzverfahren,
- die gerichtliche Ablehnung eines Insolvenzverfahrens mangels Masse,
- erfolglose oder teilweise erfolglose Zwangsvollstreckung,
- ungünstige Umstände bei Kunden mit Sitz im Ausland, die berechtigten Zweifel über die ganze oder teilweise Erfüllung der Forderung erzeugen,

Tab. 28.1 Insolvenzen in Deutschland. (Quelle: Statistisches Bundesamt 2019)

Wirtschaftsabschnitt	Insolvenzen	
	2017	2018
Unternehmen (einschließlich Kleingewerbe)	20.093	19.302
Einzelne relevante Wirtschaftsabschnitte		
Handel; Instandhaltung und Reparatur von Kraftfahrzeugen	3627	3285
Baugewerbe	3298	3334
Verkehr und Lagerei	1319	1269
Verarbeitendes Gewerbe	1592	1402

- der „Protracted Default“ als Nichtzahlungstatbestand. Er tritt in aller Regel nach sechs Monaten Zahlungsverzug eines nicht insolventen Kunden ein. Die Frist beginnt ab Meldung des Zahlungsverzugs durch den Versicherungsnehmer.

28.3.2.2 Marktübliche Bedingungen und Klauseln für die Warenkredit-Versicherung

Bis zur Aufgabe der materiellen Bedingungsaufsicht durch das BaFin im Jahre 1994 war die Versicherung von Warenkrediten in Deutschland durch einheitliche Bedingungswerke geprägt: die „AVB WKV 1984“ zur Warenkreditversicherung und die „AVB AKV 1984“ zur Ausfuhrkreditversicherung. Die Versicherer haben seither vor allem aus Wettbewerbsgründen die Bedingungskonditionen verändert, um sich von Marktmitbewerbern abzuheben. Das erschwert die Vergleichbarkeit. Jedoch hat sich der Gegenstand der Versicherung nicht tief greifend verändert. Per Klausel können Besonderheiten des Deckungsbedarfs im Versicherungsschutz berücksichtigt werden (vgl. Gerling 2007, S. 118).

28.3.2.3 Gegenstand der Versicherung und Deckungsformen

„Der Versicherungsschutz erstreckt sich auf Forderungen, die während der Laufzeit des Versicherungsvertrages entstehen und die wegen eines ebenfalls während der Laufzeit des Versicherungsvertrages bei einem versicherten Kunden eingetretenen Versicherungsfalles ausfallen“ (vgl. Euler Hermes SA 2008, S. 1). Der Versicherungsschutz beginnt ab Versendung „(...), sofern die Forderungen aus dieser Lieferung und der Leistungen innerhalb der nächsten 30 Kalendertage fakturiert werden.“

Die Entschädigung beläuft sich auf den Fakturawert exklusive Mehrwertsteuer. Hier von werden folgende Positionen abgezogen:

- nicht versicherte Forderungen,
- aufrechenbare Forderungen,
- Erlöse aus der Verwertung von Sicherheiten (Eigentumsvorbehalt),
- Erlöse aus sonstigen Rechten und Sicherheiten und
- Rückflüssen aus der Insolvenzquote sowie eine
- „spürbare“ Selbstbeteiligung.

Die Vereinbarung der Versicherungssumme beruht auf einer Bonitätsprüfung. Der Versicherungsnehmer muss eine ausreichend hohe Versicherungssumme für alle Forderungen gegen seine Kunden, innerhalb eines bestimmten Zahlungsziels, beantragen. Sobald eine Gesamtforderung die Antragsgrenze, zum Teil auch „Anbietungsgrenze“ genannt, erreicht, muss dies beim Versicherer angezeigt werden (vgl. Euler Hermes SA 2008, S. 3). Bei schwieriger Bonitätslage verlangt das Versicherungsunternehmen Maßnahmen zur Sicherung der Forderung oder zeichnet ein niedrigeres, im ungünstigen Fall kein Limit. Denkbar ist auch die Vereinbarung von kürzeren Zahlungszielen.

Das äußerste Zahlungsziel, auch Kreditlimit genannt, bildet den Zeitraum, in dem der Versicherungsnehmer eine Zahlung abgewickelt haben muss. Wird es überschritten, muss er dies dem Versicherer anzeigen, ansonsten gefährdet er seinen Versicherungsschutz.

In einer Vordeklaration hat der Versicherungsnehmer sein Debitorenmanagement darzulegen. Es kann eine Anbietungsgrenze (oder Selbstprüfungsgrenze) vereinbart werden, bis zu der alle Forderungen versichert sind. Sobald die Anbietungsgrenze überschritten wird, ist der Versicherungsnehmer angehalten, die Festsetzung der Versicherungssumme beim Versicherungsunternehmen zu beantragen.

Die Höchsthaftung p. a. wird häufig mit dem Zwanzig- bis Vierzigfachen der Jahresnettoprämie vereinbart. Wird diese überschritten, sollte der Versicherungsnehmer gegen Prämie eine höhere Höchsthaftung versichern (vgl. Gerling 2007, S. 117 ff.).

Entstandene Kosten für Güter, die nach ihrer Bestellung hergestellt werden, bergen das sogenannte Fabrikationsrisiko. Das Risiko besteht einerseits aus der Unwagbarkeit des Exporteurs, dass die Fertigung oder der Versand der Ware durch höhere Gewalt verhindert wird oder unzumutbar ist. Andererseits kann auch die Zahlungsunfähigkeit des Importeurs als Risiko definiert werden. Dieses Risiko kann regelmäßig im Rahmen der Fabrikationsrisiko-Klausel eingeschlossen werden. Gleches gilt, wenn eine Auslieferung der Güter auf Weisung des Versicherers (zum Beispiel infolge einer Gefahrerhöhung) unterbleibt. Auch dann ist der Kreditversicherer für die entstandenen Selbstkosten regelmäßig eintrittspflichtig.

Die Kreditversicherung bietet dem Versicherungsnehmer eine Alternative zum Factoring, welches den Verkauf von Forderungen vorsieht (vgl. IHK Köln 2017, S. 3).

28.4 Verlustprävention

Um Risiken zu minimieren, stehen Unternehmen vor dem Abschluss eines Versicherungsvertrages einige weitere Methoden zur Verfügung. Eine wirksame Methode, um Risiken im Zusammenhang mit dem Transport von Gütern zu verringern, ist, Schäden durch aktives Riskmanagement vorzubeugen.

28.4.1 Beanspruchung der Güter während des Transports

In einem Kaufvertrag wird definiert, welches Gut, in welcher Menge und in welchem Zustand es zu seinem Bestimmungsort transportiert werden soll. Wer Sorge für den Transport zu tragen hat, wird in den Lieferbedingungen festgelegt. Die Waren werden während des Transports verschiedenen Kräften ausgesetzt. Die Beanspruchung des Gutes ist von verschiedenen Einflussfaktoren abhängig, zum Beispiel: Transportmittel, Route, Verpackung, Beschaffenheit des Gutes, Umwelteinflüsse oder Zwischenlagerung. Der CTU-Code, herausgebracht von der internationalen Seeschifffahrts-Organisation (IMO), der Internationalen Arbeitsorganisation (ILO) und der Wirtschaftskommission der Vereinigten

Nationen für Europa (UNECE), ist eine Verhaltensregel mit dem Ziel, dem Verantwortlichen für das Packen und Sichern Hinweise und einen Überblick über die theoretischen Details der Ladungssicherung zu geben. Sie definiert eine CTU (Cargo Transport Unit) als Beförderungseinheit, zum Beispiel einen Frachtcontainer, einen Wechselbehälter, ein Transportfahrzeug oder einen Wagen.

Der ISO-Container (ISO = Internationale Organisation für Normungen) ist ein Universalbehälter, der durch Normen und eine Zulassungsprüfung der CSC (Convention for Safe Containers) eine international festgelegte Abmessung aufweist. Die laufende Prüfung der Container wird durch die CSC-Plakette nachgewiesen, die ihre Gültigkeit bei einer Beschädigung des Containers verliert. Die Standardcontainer sind aus Corten-Stahl, der nicht anfällig für Korrosion ist. Der Frachtcontainer als solches ist für vergleichsweise leichte Ladung ausgelegt, die sich auf den gesamten Containerinnenraum gut aufteilt. Der Frachtcontainer ist dank seiner stabilen Beschaffenheit für die wiederholte Verwendung ausgelegt (vgl. GDV 2016, S. 26 ff.). Für schwereres Transportgut ist eher das Großpackmittel geeignet. Es ist eine starre, halbstarre oder flexible transportable Verpackung mit einem Fassungsvermögen von bis zu 3000 l für feste oder flüssige Stoffe, die für mechanische Handhabung ausgelegt ist und der Beförderung standhält. Ein Wechselbehälter ist eine CTU, die für den kombinierten Verkehr (Schiene/Straße) gefertigt worden ist. Dafür sind mindesten vier Beschläge für die Befestigung von Drehverschlüssen nach ISO-Norm 1161-1983 vorgesehen, um den Unterboden an verschiedenen Vehikeln befestigen zu können (vgl. TIS 2019a).

Häufige Fehler bei der Verwendung von Containern sind die zu hohe Stapelung oder der Transport von schweren Gütern mit hoher Punktbelastung, woraus häufig hohe Schäden resultieren (vgl. GDV 2016, S. 26 ff.). Ebenfalls sind es nicht hinreichend kraftschlüssige Verbindungen zwischen Gütern und Containern, zum Beispiel durch eine fehlende Verblockung von Zwischenräumen, die schwerwiegende Folgen haben können. So zieht das Containerhandbuch zu diesem Thema einen beispielhaften Fall heran, in dem bei einem kombinierten Transport hoch gestapelte Schaltschränke und Maschinen nicht kraftschlüssig gestaut und mangelhaft gegen die Einwirkung seitlicher Beschleunigung (beispielsweise durch „Lasching“) gesichert wurden. Durch die nachlässige Lagerung sind Maschinenteile gegen die Containerwand geworfen worden und haben diese beschädigt (vgl. TIS 2019a).

28.4.1.1 Mechanische Beanspruchung

Wenn man von mechanischer Beanspruchung spricht, differenziert man je nach Belastungsdauer und -häufigkeit zwischen mechanisch-statischer und mechanisch-dynamischer Belastung. Welche Beanspruchung in welcher Intensität zu erwarten ist, hängt maßgeblich von dem gewählten Transportmittel, der Umschlagshäufigkeit und dem Reiseweg des Gutes ab.

Mechanisch-statische Beanspruchung entsteht durch über einen langen Zeitraum auf das Gut einwirkende Gewichtskräfte. Typisch für mechanisch-statische Belastung ist die

Stapel Lagerung. Hier sind durchschnittliche Stapelhöhen, wenn das Gut grundsätzlich stapelbar ist, zwischen drei und sechs Metern üblich.

Mechanisch-dynamische Beanspruchung entsteht bei häufigeren, kurzen Krafteinwirkungen, etwa durch Beschleunigung, Fallen, Stoßen oder Schwingung. Die Beschleunigungs Kräfte können mit der Einheit „g“ (Erdbeschleunigung „g“ entspricht $9,81 \text{ m/s}^2$) beschrieben werden. Transportgüter können je nach Beschaffenheit unterschiedlich intensive Beschleunigungsvorgänge, wie zum Beispiel Fallen oder Stoßen, unbeschadet überstehen. Die Verpackung von Transportgütern soll deren Belastbarkeit soweit erhöhen, dass sie den gewöhnlichen Beanspruchungen während der Beförderung, Lagerung und des Umschlags gewachsen sind und keinen Schaden durch die oben beschriebenen Krafteinwirkungen nehmen. Bei der Berechnung der Ladungssicherung werden die verschiedenen Krafteinwirkungen berechnet. Je nach Transportmittel unterscheiden sich die mechanisch-dynamischen Beanspruchungen, zum Beispiel aus Anfahrdruck, Kurven, Rangieren, Abbremsen, Seegang oder Vibration. Während eines Lkw-Transports ist das zu befördernde Gut lang anhaltender Vibration ausgesetzt. Dessen Intensität hängt von der Beschaffenheit des Fahrbahnuntergrunds ab. Sie muss durch stabile Außenverpackung und stoßdämpfende Innenverpackung berücksichtigt werden. Bei Bahntransporten sind die höchsten Beschleunigungswerte durch Rangierstöße zu erwarten. Hier wirken je nach Zugstrecke und Schienennetz zwischen 4 g und 16 g ein. Auf See ist die Ware je nach Stauplatz starken vertikalen Bewegungskräften (2 g) durch Wellentäler ausgesetzt. Hierbei entstehen auch horizontale Beschleunigungen (0,8 g) durch Rollbewegungen des Schiffes. Bei rauer See können diese lange und intensiv auf die Ware einwirken. Beim Lufttransport kann es in Spitzen durch Luflöcher oder Landen zu hohen dynamischen Beanspruchungen (2,5 g) kommen (vgl. Gerling 2007, S. 141 f.).

Im Fall multimodaler Transporte, mit verschiedenen Transportmitteln und Güterumschlägen, muss die Verpackung und Ladungssicherung den höchsten Belastungswerten entsprechend gewählt werden. Dabei unterscheidet man zwischen Direktsicherung, Reibungssicherung und Kompaktieren. Die Direktsicherung, zum Beispiel durch „Lasching“, ist vorzugsweise anzuwenden. Sie sichert mit Gurten und Blockaden in die Richtung, in welche die Bewegungskraft wirkt. Die Reibungssicherung ist nur für kleine Teile in einem Container zu empfehlen, hier wird das Gut mit Laschen auf dem Boden gezurrt. Die Vorspannung ist hierbei entscheidend, geht sie verloren, ist die Sicherung wirkungslos. Durch Kompaktieren können viele kleine Teile zum Beispiel mit Schrumpffolie auf einer Palette fixiert werden. Dann muss man nicht mehr einzelne kleine Teile, sondern eine große Palette sichern (vgl. GDV 2016, S. 254 f.).

28.4.1.2 Klimatische Beanspruchung

Die Einwirkungen des Klimas machen sich an Umschlag- und Lagerplätzen besonders bemerkbar. Je nach Reiseroute und Reiseziel variiert dort die Beanspruchung durch die lokale Wetterlage. Transportmittel wie Eisenbahn oder Schiff durchqueren oft mehrere Klimazonen. Niederschläge und Luftfeuchtigkeit sowie starke Temperaturschwankungen können zu starker Beanspruchung durch Kondenswasserbildung führen. Bei diesem Phänomen bildet sich auf den Wänden von LKW und anderen Transportmitteln ein dicker Wasserschicht, was die Beladung und die Transportmittel beschädigen kann.

nomen differenziert man zwischen Ladungs- und Containerschweiß. Bei starken Schwankungen von höherer zu niedrigerer Temperatur kommt es zu Kondensat an der Containerdecke oder -wand. Hier sollte auf entsprechende Folierung des Containers und die entsprechende Platzierung des Gutes möglichst ohne direkten Kontakt zur Innenwand des Containers geachtet werden.

Ladungsschweiß entsteht durch einen Anstieg der Luftfeuchte und eine extrem hohe Außentemperatur. Gewöhnlich ist die Außentemperatur jedoch niedriger als die Containerrinnentemperatur, wodurch die Luftfeuchte verringert wird, wenn Außenluft eindringt. Die Luftfeuchte selbst ist abhängig von den hygroskopischen Eigenschaften von Ladung, Verpackung und Beipackmaterialien. In Abhängigkeit mit der bestehenden relativen und absoluten Luftfeuchte besitzt die Luftmasse einen Taupunkt, welcher bei einer bestimmten Temperatur erreicht wird. Hier kondensiert Wasser an der kühleren Ladung. Dieses Phänomen muss insbesondere bei der Wahl der Verpackung und Lagerung zum Beispiel mit der Sperrsichtmethode berücksichtigt werden.

Im Gegensatz zum Standard-Container herrscht in passiv belüfteten Containern (sogenannte Kaffeecontainern) die gewünschte Luftzirkulation, um die Abkühlung der Ware zu erreichen. Der Kühl-Container hat eine bessere Isolierung und somit einen geringeren Wärmedurchgangswert der Wände. Temperaturschwankungen des Außenklimas haben dementsprechend geringere Auswirkungen. Der offene Container besitzt so gut wie kein eigenes Containerklima. Das Außenklima bestimmt die Temperatur (vgl. TIS 2019d).

28.4.2 Vorbeugender Transportschutz

Der benötigte vorbeugende Transportschutz bezieht den gesamten Beförderungsprozess und die Empfindlichkeit der Ladung in die Überlegungen über die Auswahl des Packmittels und seiner Menge ein. Ebenfalls müssen Reiseroute, -ziel, Be- und Entladevorgänge, Zwischenlagerungen und Nachreise berücksichtigt werden. Sind Seetransporte geplant, muss die Verpackung den Beanspruchungen der Seebeförderung standhalten, also „seemäßig“ sein. Nachdem ein Gut im Zielhafen ausgeladen wurde, folgen häufig noch Umschläge auf dem Landweg. Hier entstehen regelmäßig größere Beanspruchungen durch die Verladung, denen die Verpackung ebenfalls standhalten muss (vgl. Gerling 2007, S. 147).

Die **Außenverpackung** ist überwiegend in die Materialien Holz, Pappe und Textil ein teilbar. Holz ist gut geeignet als Außenverpackung, da es bei hoher Stabilität und Biegsamkeit relativ leicht ist. Häufig genutzte Holzarten sind Vollholz und Nadelholz. Die notwendige mechanische Beanspruchbarkeit und Qualität wird durch DIN-Norm 4074 T1 vorgegeben. Der Holzwerkstoff kann unverarbeitet zur Verschalung von Transportgütern genutzt werden. Es kommen aber auch verarbeitete Holzwerkstoffe wie Holzfaser-, Span- und Sperrholzplatten zum Einsatz. Diese Holzwerkstoffe bedürfen in Hinblick auf die Verarbeitung und Verleimung des Holzes besonderer Sorgfalt. Denn die gesamte Verpackung muss allen gewöhnlichen Witterungen und Belastungen standhalten können. Den

verschiedenen Holzwerkstoffen wurden DIN-Normen zur Sicherung der Qualität zu grunde gelegt.

Aus Holzwerkstoffen werden Kisten, Verschläge und Teilverpackungen hergestellt. Die Kiste schützt das Transportgut gegen schädigenden, äußeren Kontakt. Zusätzlich zu der normalen Wandung sind am Boden Quer- und Längskufen und am Deckel Deckelhölzer angebracht, um die Belastbarkeit der Kistenkonstruktion zu erhöhen. Die Stärke der einzelnen Komponenten hängt von den zu transportierenden Produkten ab. Der Verschlag hingegen ist eine durchlässige Außenverpackung mit unterschiedlicher Stabilität gegen Druckbelastung, je nach Konstruktion.

Teilverpackungen sind beispielsweise Kantholzkonstruktionen (vgl. Abb. 28.1), Schlitzen, Verschalungen (vgl. Abb. 28.2) oder der Bund.

Schachteln werden als Konsumverpackung (Vollpappe) aber auch als Transportverpackung (Wellpappe) genutzt. Die Festigkeit der Pappe hängt grundsätzlich von der flächenbezogenen Menge an verarbeitetem Material ab. DIN-Norm 55468-1 legt fest, welche Qualitätsstandards die Pappe erfüllen muss. Hier ist zusätzlich die Art und Menge an Welleneinzügen zwischen den Deckblättern maßgeblich für die Stabilität der Pappe. Die Wellpappenqualität leidet unter hohen Luftfeuchten (vgl. Gerling 2007, S. 148 ff.).

Als Transportpackmittel zum Schutz gegen Staub oder Feuchte werden Faltschachteln aus Wellpappe verwendet. Der „Box-Compressive-Test“ ermittelt die Tragfähigkeit einer Schachtel durch Belastung des Materials, bis es einknickt. Der BMC-Wert ist bei kleineren Kisten höher (besser) und wird durch einen verstärkten Kantenstauchwiderstand weiter erhöht (vgl. Gerling 2007, S. 158).

Fässer und Kanister können an sich durch formschlüssige Stauung eine stabile Ladungssicherung herstellen. Bei dem Gefahrenguttransport mit Fässern ist darauf zu achten, dass diese stets aufrecht verstaut werden. Je nach Größe der Fässer können diese entweder in gleichmäßigen Reihen im sogenannten „Soldatenstau“ (kann bei größeren Fässern vorteilhaft sein) oder vertikal gestapelt, „versetzt verstaut“, werden (vgl. Gerling 2007, S. 171).

Die **Innenverpackung** ist sorgsam auszuwählen und sollte ausgehend vom Transportgut und den Transportbedingungen bestimmt werden. Sie soll die Transportgüter gegen die mechanischen und klimatischen Beanspruchungen des Transports schützen. Geeignete Staumaterialien zum Schutz vor Kondenswasser sind Holzbretter am Boden der CTU, wasserziehende Textilien wie Sackleinen gegen an der Decke kondensierendes Wasser oder Sperrholz gegen Wasser, dass sich an den Seitenwänden der CTU bildet. Es ist darauf zu achten, dass die natürliche Belüftung erleichtert wird indem Lücken in der Ladungskonstruktion vorgesehen werden. Um die mechanische Belastung in Stapeln von Versandstücken auszugleichen, ist es wichtig, diese durch Paletten zu fixieren und sie durch Sperrhölzer zu trennen.

Grundsätzlich ist für den Packvorgang von Kartons oder schweren Einheiten eine reibungsarme Oberfläche besser geeignet als Packmittel mit erhöhtem Reibwert, wie zum Beispiel Säcke. Jedoch fordert eine hohe Reibung innerhalb der Güter (Pulver oder Granulat) oder der einzelnen Versandstücke, wie zwischen in Säcken verstauten Versandstücken.

Abb. 28.1 Kantholzkonstruktion, Drei-Weg-Eck. (Quelle: eigene Darstellung in Anlehnung an TIS 2019f)

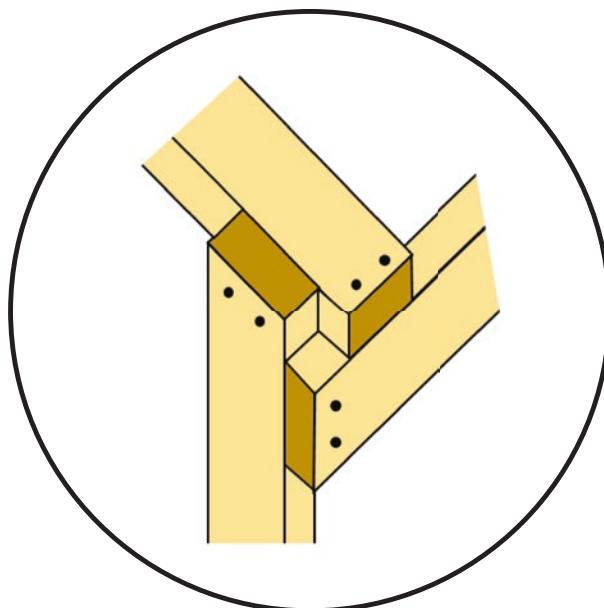
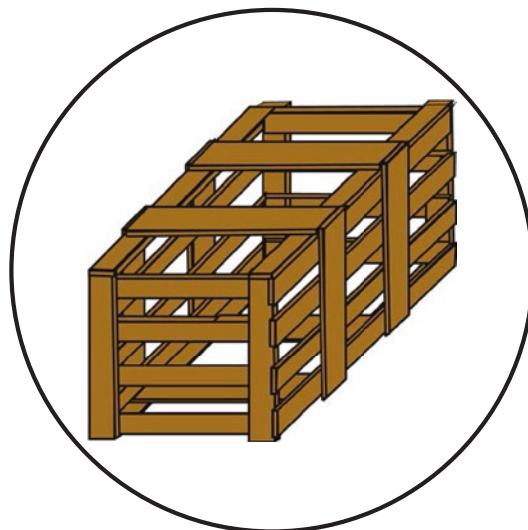


Abb. 28.2 Verschalung.
(Quelle: eigene Darstellung in Anlehnung an TIS 2019f)



cken, eine stabile Stauung. Insbesondere hat die Reibung zwischen der Ladung und dem Staubboden einer CTU in diesem Zusammenhang positiven Einfluss auf die Ladungssicherung. Die Intensität der vertikalen Reibungskräfte ist gleich dem Zusammenhang aus spezifischen Reibwert μ der Masse des Gegenstands und dem vertikalen Beschleunigungskoeffizienten: Reibungskraft $FF = \mu \cdot cz \cdot m \cdot g$ [kN], mit der Ladungsmasse [t] und $g = 9,81$ [m/s²]. So kann die statische Reibung zwischen verschiedenen Oberflächenmaterialien bemessen und diese dann auf die für die Ladung verwendete Verpackung bezogen

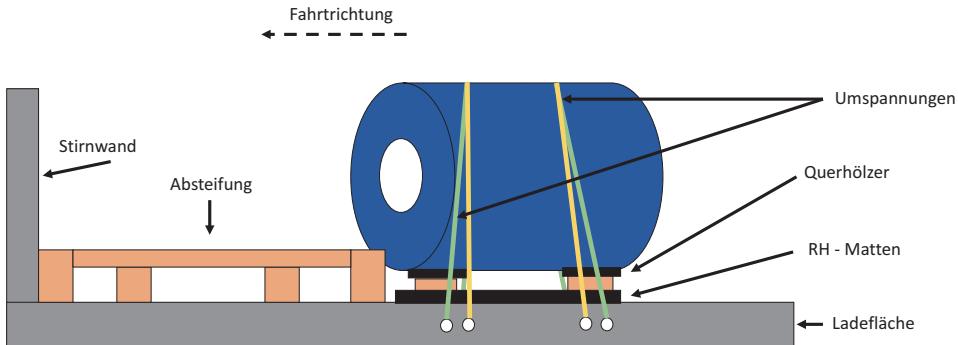


Abb. 28.3 Absteifung. (Quelle: eigene Darstellung in Anlehnung an TIS 2019c)

werden. Die Informationen zu der Verwendung von reibwerterhöhenden Materialien sowie die Tabelle der jeweiligen Reibwerte sind den CTU – Packrichtlinien zu entnehmen (vgl. Bundesministerium für Verkehr und digitale Infrastruktur 2015, S. 98).

Um die während des Transports entstehenden Drücke abzufangen und zu übertragen, werden die Methoden **Blockieren**, **Ab- oder Aussteifen** verwendet (vgl. Abb. 28.3.) Holzbalken, Holzrahmen, Paletten oder Staupolster werden in Lücken zwischen den verschiedenen Versandstücken eingefügt. Um der Druckübertragung durch die Ab- oder Aussteifung standzuhalten, muss der Druck an den Kontaktstellen durch Querträger oder ähnliches verteilt werden, außer das Bauelement ist in sich stabil. Damit die Konstruktion bei vorübergehendem Druckverlust auch weiterhin intakt bleibt, muss sie durch Diagonalstreben, geeignete Pfosten, verkeilt und fixiert werden. Zur Bewertung der Vorrichtungen wird die nominale Holzfestigkeit genutzt. Eine detaillierte Übersicht findet sich in den CTU-Packrichtlinien.

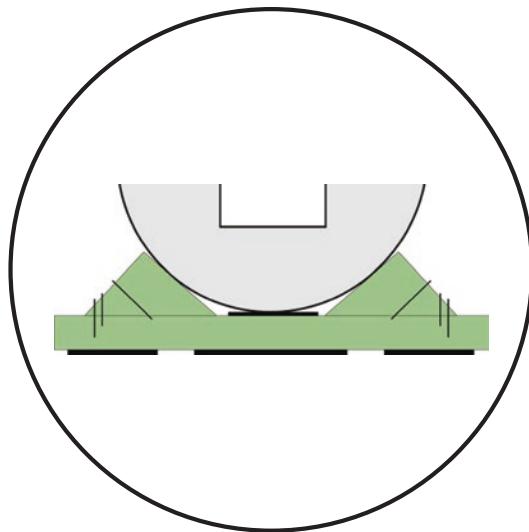
Bei geringerer Anforderung an die Ladungssicherung können Transporteinheiten durch aufgenagelte **Kanthölzer** blockiert werden (vgl. Abb. 28.4). Die Keile sollten so gesägt sein, dass die Scherfestigkeit durch die Richtung der Maserung erhöht wird. Die Keile sollten auf unter der Ladung gelegene Staumaterialien genagelt werden. Runde Körper, wie zum Beispiel Rohre, können durch diese Methode fixiert werden (vgl. Bundesministerium für Verkehr und digitale Infrastruktur 2015, S. 95 ff.).

Wird die Ware formschlüssig verstaut, so ist jede Lücke mit geeignetem Staumaterial, dass sich nicht dauerhaft verformt, auszufüllen. Horizontal ist in Summe 15 cm Lücke als Obergrenze festgelegt. Lücken zwischen auf Paletten verzurrtten oder fixierten Transportgütern können vernachlässigt werden. Bei der Verwendung von Staukissen muss auf die Herstellerhinweise bezüglich der Belastbarkeit und die maximalen Spaltbreite des Staumaterials geachtet werden.

Die **Markierung** eines Packstückes ist von hohem Stellenwert, um eine adäquate Handhabung sicherzustellen. Mit einer präzisen, prägnanten und permanenten Markierung können Unfälle, Falschauslieferung, Verluste und Zollstrafen vermieden werden.

Dabei hat sich die Markierung schwarz auf weißem Untergrund allgemein durchgesetzt. Die Markierung muss aus der Leitmarke, der Informationsmarkierung und den Handhabungshinweisen bestehen. Die Leitmarke umfasst die Kennmarke (Initialen des

Abb. 28.4 Kanthölzer. (Quelle: eigene Darstellung in Anlehnung an TIS 2019c)



Empfängers), seine Auftragsnummer, die Anzahl der Packstücke, die laufende Nummer des entsprechenden Packstückes innerhalb der Sendung und den Bestimmungsort. Die Informationsmarkierung gibt das Ursprungsland, eine Gewichtsangabe und die Abmessung des Packstücks an. Zum Zwecke des sorgfältigen Transports werden Handhabungshinweise an das Packstück gebracht. Sie sind nach ISO R/780 und DIN 55 402 international einheitlich festgelegt. Sie geben darüber Auskunft, ob das Packstück hitze- oder nässeempfindlich, bruchgefährdet, an welcher Stelle die Schwerpunktllage ist und an welcher Ecke das Ladegeschirr angebracht werden kann (vgl. TIS 2019e).

Zurmaterialien und -einrichtungen übertragen Zugkräfte. Zurmittel sollten entsprechend ihres Einsatzgebiets eine bestimmte Bruch- und Einsatzfestigkeit haben. Die Bruch- und Einsatzfestigkeit wird maßgeblich durch die Ausprägung der Kanten und Ecken (beispielsweise von Metallverpackungen, Containern oder ähnlichem) über die sie geführt werden beeinflusst. Daher sollte ein Kantenschutz genutzt werden, um das Material zu schonen. Es gibt verschiedene Faserseile, zum Beispiel Manilafaser, Hanf, Sisal oder synthetische Materialien. Häufiger kommt auch Stahldraht in verschiedenen Formen und Einsatzfestigkeiten zum Einsatz. Weiter sollte beim Lasching auf die Vorspannung geachtet werden. Ist sie zu hoch, kann das Material bei wiederholter Dehnung dauerhaft überdehnt werden und somit seine Sicherungsfunktion verlieren (vgl. Bundesministerium für Verkehr und digitale Infrastruktur 2015, S. 102 ff.).

28.4.3 Abwehrender Transportschutz

Das Risk-Controlling während des Transports ist bei großen Ladungspartien sinnvoll, weil oft gesamte Teilbereiche von Schiffen gechartert werden. Hier können viele Risiken durch gewissenhafte Beladung des Stauraums abgewehrt werden.

Dies gelingt durch eine laufende Überwachung des Transports mit einem Transportfachmann, der das Transportgut kennt und mit dem Kapitän des Schiffes die Nutzung des Stauraums bespricht. Hierbei hat der Kapitän jedoch volle Entscheidungsgewalt über die Platzierung der Ladung, da er neben der Lagerung die Gegebenheiten auf seinem Schiff und der gewählten Seeroute berücksichtigt. Da der Transportfachmann den gesamten Transport und die Nachreise begleitet, kann er die Schadenminderung übernehmen und je nach Schadenssituation entsprechende Maßnahmen einleiten.

Die Verlustwahrscheinlichkeit ist maßgeblich vom Riskmanagement und von der Qualitätskontrolle des Spediteurs und Lagerungsunternehmens abhängig. Hier empfiehlt es sich, ein durch den Transportversicherer schriftlich festgehaltenes Maßnahmenpaket zum Zwecke der Schadenprävention zu vereinbaren. So können Organisationsverschulden vermieden und die verschiedenen Risikofaktoren kontrolliert werden (vgl. Gerling 2007, S. 182).

28.4.4 Verlustprävention in der Kreditversicherung

Lieferantenkredite entstehen auf der Basis von Kaufverträgen, die ein Zahlungsziel vorsehen. Dementsprechend erhält der Käufer das Gut, bevor es bis zum vereinbarten Zahlungsziel bezahlt wird. Es gibt zwei Gestaltungsformen: Der Buchkredit sieht eine Skonto- und eine Zahlungsfrist vor. Die Skontofrist ist kürzer und rabattiert den Kaufpreis um einen Skontoabzug. Die Zahlungsfrist sieht keine Minderung des Kaufpreises vor. Ein Wechselkredit liegt vor, wenn der Verkäufer einen Wechsel auf seinen Kunden zieht. Das Kreditinstitut wird in diesem Falle in den Kaufvertrag involviert, kauft den Wechsel, bevor das Zahlungsziel verstrichen ist, und löst somit die Verbindlichkeit ab.

Der Lieferantenkredit ist aus Sicht des Kunden äußerst vorteilhaft, weil er eine Kreditgewährung ohne systematische Kreditprüfung und eine formlose, schnelle und bequeme Abwicklung vorsieht. Außerdem ist es möglich, einen Lieferantenkredit trotz ausgeschöpfter Kreditlinie auszuhandeln (vgl. Witte 2000, S. 348). Ein möglicher Nachteil ist die Abhängigkeit von dem Lieferanten.

Aus Sicht des Kreditgebers stellt der Lieferantenkredit ein Bonitätsrisiko dar, das eingeschätzt und geprüft werden muss. Die Kosten der Bonitätsprüfung muss der Lieferant tragen. Das Risiko und die mit der Prüfung entstehenden Kosten könnten durch die Bezahlung per Vorkasse gänzlich vermieden werden. Dies erweist sich in den meisten Branchen indessen als nicht wettbewerbsfähig, deswegen kann sich die Vorkasse dort nicht durchsetzen (vgl. Göhl 2017, S. 27).

Die Informationsquellen und Sicherheiten bei der Gewährung von Lieferantenkrediten spielen bei Handelsgeschäften eine wichtige Rolle. Sie stehen jedem Unternehmen in Deutschland aber auch im Großteil des Auslands zur Verfügung. Die Auskunft erstreckt sich neben der Bonitätsbeurteilung unter anderem auf Firmierung, Anschrift, Rechtsform, Informationen über den Inhaber und die Unternehmensleitung, Gegenstand des Unternehmens oder auf Aussagen über die Entwicklung des Unternehmens.

Bonitätsprüfungen bieten Handelsauskunfteien an, zum Beispiel die Schufa. Vorteilhaft kann die Vereinbarung einer laufenden Auskunft sein, welche die Beurteilung des Kunden bei wichtigen Veränderungen aktualisiert. Sie ist jedoch nur als Grundlage einer

Kreditprüfung geeignet, da sie sich meist lediglich aus öffentlich verfügbaren Daten und Verbindungen zu Inkassounternehmen speist (vgl. Everling 2013). Weiterführende Informationen können aus Bankauskunfteien gewonnen werden. Diese umfassen allgemein gehaltene Auskünfte der jeweiligen Hausbank des Kunden über dessen wirtschaftliche Situation, Zahlungsmoral, Bonität und Geschäftsgebaren. Die Regelung der Berechtigung von Bankauskünften nach Nr. 3 II AGB Sparkassen 2018 besagt, dass Auskünfte über juristische Personen und im Handelsregister eingetragene Kaufleute dann erteilt werden dürfen, sobald sich die Anfrage auf deren geschäftliche Tätigkeit bezieht (vgl. Bruns 2018).

Inzwischen entwickeln sich einige Onlineanbieter am Markt, die eine Bonitätsauskunft anbieten. Diese Anbieter geben jedoch unterschiedliche Informationen über die jeweiligen Kriterien und die Qualität ihrer Datenerhebung preis. Sie können sich zur eigenen Recherche junger Unternehmen eignen, da diese Anbieter vergleichsweise kostengünstig arbeiten (vgl. Firmen Wissen 2019).

Durch das zivilrechtliche Abstraktionsprinzip wird durch den Übergang einer Sache vom Gläubiger an den Schuldner rechtlich letzterer Eigentümer der betreffenden Sache. Der Schuldner ist Eigentümer der in seinen Besitz übergegangenen Sache und verpflichtet sich lediglich, die eingegangene Schuld zu begleichen. Zur Absicherung eines Lieferantenkredits sichert sich der Lieferant durch eine Handelsklausel, den sogenannten Eigentumsvorbehalt ab, der den Übergang des Eigentums bei Lieferung verhindert, bis die Schuld vollständig beglichen ist. Die Pflicht zur Vereinbarung des Eigentumsvorbehalts (und dessen Erweiterungsformen) wird regelmäßig als Voraussetzung zur Versicherung des Delkredererisikos in der Warenkreditversicherung statuiert.

Der Lieferant kann dem Käufer ein Akkreditiv stellen. Dies ist eine Zahlungsbedingung, die den Risikoausgleich der Parteien durch eine Bank umsetzen lässt. Um die Erfüllungsrisiken gleichmäßig zu verteilen, kann sich der Exporteur an eine Akkreditivbank wenden. Zum Zweck der Umsetzung des Akkreditivs, werden die benötigten Frachtpapiere (Letter of Credit, kurz: L/C), die den Eigentümer der Ware legitimieren, gegen Zahlung an den Empfänger weitergegeben. Die Akkreditivbank wird angewiesen, den Kaufpreis erst bei Übergang der Frachtpapiere an den Exporteur zu zahlen. Die Eröffnung und die Abwicklung des Akkreditivs sind in den ERA („Einheitliche Richtlinien und Gebräuche für die Dokumenten-Akkreditive“) geregelt (vgl. Abb. 28.5). Diese Regeln bilden die Grundlage für alle Dokumentenakkreditive und wurden von der Internationalen Handelskammer Paris (ICC) entwickelt (vgl. Häberle 2010, S. 10).

Ein weiteres Instrument der Verlustprävention ist die Wahl sicherer Zahlungsmethoden. Im Falle einer Zahlung per Nachnahme wird dem Empfänger die Ware erst nach Zahlung des vereinbarten Betrags ausgehändigt. So kann der Lieferant sicher gehen, dass er sein Geld auch tatsächlich bekommt. Dieser Service ist jedoch vergleichsweise teuer (vgl. DHL 2019).

Die Zahlung auf Rechnung oder die Erteilung einer Einzugsermächtigung sind im Grunde sichere Methoden im Hinblick auf betrügerische Handlungen Dritter. Ist der Kunde jedoch zahlungsunfähig, kann es zum Forderungsausfall oder Verzug kommen.

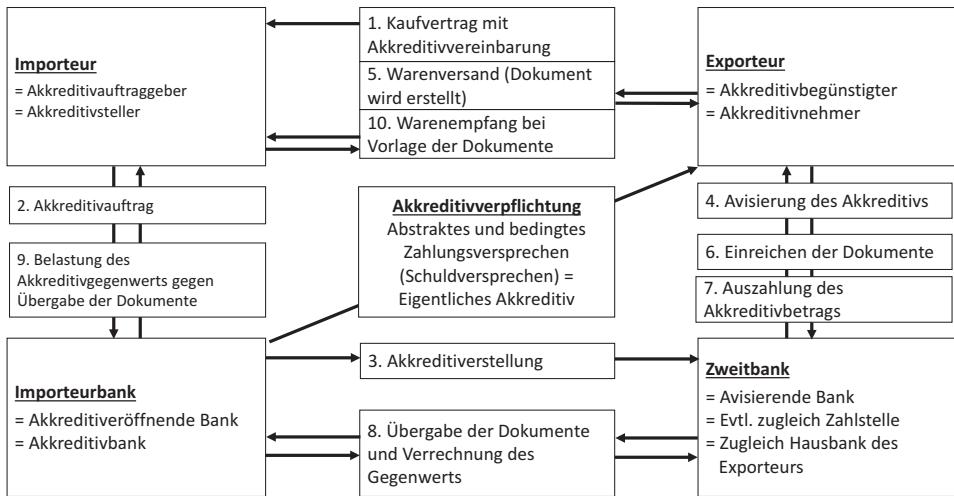


Abb. 28.5 Funktionalität des Akkreditivs. (Quelle: eigene Darstellung in Anlehnung an Häberle 2010, S. 7)

Internet-Bezahlssysteme werden seit dem 13.01.2018 von der BaFin berücksichtigt. Die Bezahlung via Internet-Bezahlssysteme ist jedoch durch verschiedene Services der einzelnen Anbieter, wie zum Beispiel Paypal, zu differenzieren. Paypal bietet mit dem sogenannten Käuferschutz die Möglichkeit, eine bereits getätigte Zahlung zurückzufordern (vgl. [Paypal 2019](#)). Kreditkarten oder Überweisungen sind insofern als sicher zu betrachten, als das Geld bereits vor Warenversand transferiert wird (vgl. [Verbraucherzentrale 2019](#)).

Die Vorkasse ist in aller Regel keine wettbewerbsfähige Zahlungsart.

28.4.5 Handlungsempfehlungen und aktuelle Entwicklungen

Beleuchtet man die aktuellen Entwicklungen der Transportversicherung, so ist in Hinblick auf die Bedingungswerte wenig Dynamik erkennbar. Schaut man jedoch auf die Marktverhältnisse, so sind durchaus Bewegungen der Prämien aufgrund jüngerer Schadenereignisse erkennbar. Um einen Fokus zu setzen, konzentriert sich dieser Beitrag auf den deutschen Markt.

In Deutschland und den angrenzenden Staaten wird ein signifikanter Anstieg von Diebstählen von Ladung, gesamten Ladungsträgern und Kraftstoff in Europa vermeldet. Im Fokus der Diebstähle stehen Waren, die eine hohe Nachfrage haben und somit umgehend weiterverkauft werden können. Die Brisanz der Situation wird durch eine Studie des Bundesamtes für Güterverkehr (BAG) aus dem Frühjahr 2017 belegt (vgl. [Bundesamt für Güterverkehr 2017](#), S. 4 ff.).

Der negative Trend wird durch die geringe Aufklärungsrate der Straftaten und ein organisiertes Vorgehen der Täter oder Tätergruppen gefördert. Hinderlich sind dabei die zeitlich nachgelagerte Ermittlung und ungeklärte Zuständigkeitsbereiche, wenn der Schadensort nicht präzisiert werden kann. Das Tatortprinzip erschwert in diesen Fällen die Polizeiarbeit.

Die „Arbeitsgemeinschaft Diebstahlprävention in Güterverkehr und Logistik“ hat einen Maßnahmenplan erarbeitet, der zur Minderung und Vorbeugung von Ladungsdiebstählen umgesetzt werden soll. Zu diesen Maßnahmen gehören die vollständige Erfassung der Diebstähle von Ladung in einer selbstständigen Kategorie der polizeilichen Kriminalstatistik, die länderübergreifende Strafverfolgung, Gründung einer Polizeieinheit zur Verfolgung von Ladungsdiebstählen oder die vereinfachte Anzeigerstattung in Fällen von Ladungsdiebstahl (vgl. TIS 2018). Weitere Vorschläge sind die Einrichtung gesicherter Lkw-Parkplätzen oder die Errichtung eines länderübergreifenden Risk-Managements in Speditionen, die im Rahmen der Schadenverhütungstagung 2019 des GDV diskutiert und zur Umsetzung unterbreitet wurden (vgl. TIS 2019b).

In der Agenda dieser Tagung wurde auch auf die Möglichkeiten der Verlustprävention seitens der Versicherungsnehmer hingewiesen. So können Kosten in der Lieferkette minimiert werden, wenn Schadenverhütungsmaßnahmen umgesetzt werden. Mögliche Maßnahmen sind das Tracking & Tracing der Ware. Hier werden durch Location-Based-Technologien, wie GPS Standortdaten des Verkehrsträgers oder der Ware selbst, an das Überwachungsunternehmen übermittelt. Zur Überwachung von Umschlagplätzen eignet sich die Videoüberwachung von Abstellplätzen der Transportfahrzeuge oder der Zwischenlager.

Ware kann durch künstliche DNA markiert werden, um sie im Falle eines Diebstahls wiedererkennen zu können.

Gegen sogenannte „Planenschlitzer“ helfen verschiedene Alarmanlagen, die den Nutzer per Mail und SMS informieren, falls ein potenzieller Dieb das ausgestattete Fahrzeug beschädigt (vgl. Theftex 2019). Die mechanische und elektronische Sicherung der Frachtcontainer sowie die Innenraumüberwachung sind ebenfalls Abwehrmaßnahmen, die als Diebstahlschutz in Betracht gezogen werden sollten (vgl. TIS 2019b).

28.5 Fazit

Die Absicherung eines Lieferantenkredits und eines Warentransports wird aus versicherungstechnischer Perspektive grundsätzlich getrennt behandelt. Dennoch sollte ein einheitlicher Risikomanagementprozess für die Aufnahme und Umsetzung von Handelsbeziehungen aufgesetzt werden.

Die konkreten Maßnahmen der Verlustprävention sind vom Versicherungsnehmer als Grundlage zu betrachten. Die Vorkehrungen sollten transport- und branchenspezifisch getroffen werden. Befinden sich Unternehmen im Wachstum und haben eine hohe Abhängigkeit von Neukunden, deren Bonität bisher unbekannt ist, ist ein funktionierendes Kreditprüfungs- system unabdinglich, um einen langfristigen Geschäftsbetrieb zu sichern und vor Insolvenz aus Forderungsausfall zu schützen. Risikosituationen, wie eine signifikante Fremdkapitalquote oder eine hohe Abhängigkeit von wenigen Kunden, sollten durch ein hochwertiges Risikomanagementkonzept gedämpft werden.

Ferner sind die verschiedenen Maßnahmen des vorbeugenden Transportschutzes notwendig, um ein nachhaltiges Transportwesen zu betreiben. Hierbei sollten verschiedene Kon-

trollinstanzen, periodisch bis kontinuierlich, die Angemessenheit der Verpackungsmaterialien und Sicherungsmethoden prüfen. Ist das Risikomanagement mit dem Transportversicherer abgestimmt, spricht dies für eine hochwertige Kundenbeziehung und vermittelt dem Versicherer eine risikobewusste Unternehmensführung (vgl. Gerling 2007, S. 182).

Konzeptionell wird der Versicherungsschutz auf einen funktionierenden Risikomanagementprozess aufgesetzt. Wie in den Kapiteln dargestellt, lässt sich die Deckung dem Bedarf der versicherten Unternehmen bis zu einem gewissen Grad anpassen. Mit Blick auf die sich im Zeitablauf ändernden vorherrschenden Risikoverhältnisse ist es sinnvoll, den Versicherungsschutz kontinuierlich auf dessen Angemessenheit hin zu untersuchen und den Ergebnissen entsprechend zu handeln.

Insbesondere bei der Erschließung neuer Geschäftsfelder ist es sinnvoll, die bestehenden Versicherungskonzepte und verwendeten Methoden kritisch auf Adäquanz und Wirksamkeit zu prüfen. Hierbei sollten die aktuellen Entwicklungen der Technik niemals außer Acht gelassen werden, um die bestmögliche Vorsorge für die geplante Geschäftsbeziehung und den laufenden Betrieb zu erreichen.

Literatur

- Brunn, P. (2018). Gabler Banklexikon, Das Wissen der Experten. <https://www.gabler-banklexikon.de/definition/bankauskunft-55943/version-339848>. Zugegriffen am 05.06.2019.
- Bundesamt für Güterverkehr. (2017). *Diebstähle im Transportbereich -Aktualisierte Fassung (Marktbeobachtung Güterverkehr)*. Köln.
- Bundesministerium für Verkehr und digitale Infrastruktur (Hrsg.). (2015). *Verfahrensregeln der IMO/ILO/UNECE für das Packen von Güterbeförderungseinheiten, CTU-Code*. Dortmund: Sonderdruck des Verkehrsblatt.
- DHL. (2019). Privatkunden, Service Nachnahme. <https://www.dhl.de/de/privatkunden/information/service-nachnahme.html>. Zugegriffen am 14.08.2019.
- Ehlers, H. C. (2001). *DTV-Gütersicherungsbedingungen 2000: (DTV-Güter 2000); Erläuterungen und Kommentierung, zugleich ein Vergleich mit den ADS-Gütersicherung 1973/94 und den einschlägigen Vorschriften der ADS 1919*. Karlsruhe: VVW.
- Euler Hermes, S. A. (2008). *Schutz vor Forerungsausfall: Allgemeine Versicherungsbedingungen für die Warenkreditversicherung* (Allianz (Hrsg.)). Allianz.
- Everling, O. (2013). „Rating – Chance für den Mittelstand nach Basel II: Konzepte zur Beurteilung von Bonität Schlüssel zur Finanzierung. Wiesbaden: Springer.
- Firmen Wissen. (Hrsg.). (2019): Startseite. <https://www.firmenwissen.de/index.html>. Zugegriffen am 26.07.2019.
- Gerling Konzern (Hrsg.). (1985). *Warenhandel und Versicherung*. Köln: Gerling Konzern.
- Gerling Konzern. (Hrsg.). (2007). *Güter in Bewegung – Sicherung und Risiken: Warentransport und Warenkreditversicherung Claims- und Riskmanagement Handeln in weltweiten Netzwerken*. Köln: Gerling Konzern.
- Gesamtverband der Deutschen Versicherungswirtschaft e. V. (Hrsg.). (2016). *Schadenverhütung 2016: Container*, Bremerhaven, 17.–20.04.2016, Berlin.

- Göhl, A. (2017). *Die Kreditversicherung: Grundlagen und Praxis*. Karlsruhe: VVW GmbH.
- Häberle, S. G. (2010). *Handbuch der Akkreditive, Inkassi, Exportdokumente und Bankgarantien, Arten, Abwicklungen, Fallbeispiele, Problemlösungen, Prüflisten, Richtlinien und Kommentare*. München/Wien: R. Oldenbourg.
- IHK-Köln. (Hrsg.). (2017). Lieferantenkredite und Kreditversicherungen. https://www.ihk-koeln.de/upload/Merkblatt_Lieferantenkredite_und_Kreditversicherungen_29193.pdf. Zugriffem am 06.08.2019.
- Paypal. (2019). Was ist der PayPal-Käuferschutz? So funktioniert der Käuferschutz. <https://www.paypal.com/de/webapps/mpp/paypal-safety-and-security>. Zugriffem am 08.08.2019.
- Statistisches Bundesamt. (2019). Gewerbemeldungen und Insolvenzen, Insolvenzen und Insolvenzhäufigkeiten von Unternehmen. <https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Unternehmen/Gewerbemeldungen-Insolvenzen/Tabellen/wirtschaftszweige2008.html>. Zugriffem am 05.06.2019.
- Suhr, A. (2017). *Transport und Versicherungsspeditionsrecht*. Hagen: Hagener Wissenschaftsverlag.
- Theftex. (2019). Solutions, For tarpaulin superstructures. <https://www.theftex.com/en/solutions-for-tarpaulin-superstructures/>. Zugriffem am 16.08.2019.
- Tittko, H. (2015). Die „beanspruchungsgerechte“ Verpackung in der Transportversicherung. *Die VersicherungsPraxis*, 2015(8). Gesamtverband der versicherungsnahmenden Wirtschaft e. V., Bonn, (Hrsg.).
- Transport-Informations-Service. (Hrsg.). (2018). Maßnahmen gegen Ladungsdiebstähle. http://www.tis-gdv.de/tis/bedingungen/ladungsdiebstaehte/mgd_tis.pdf. Zugriffem am 08.06.2019.
- Transport-Informations-Service. (Hrsg.). (2019a). Containerhandbuch, 21 ADS 1973/1994. http://www.containerhandbuch.de/chb/rueh/index.html?/chb/rueh/rueh_21_07.html. Zugriffem am 28.08.2019.
- Transport-Informations-Service. (Hrsg.). (2019b). Diebstahlprävention beim Warentransport auf der Straße. <http://www.tis-gdv.de/tis/tagungen/svt/svt19/inhalt.htm>. Zugriffem am 16.08.2019.
- Transport-Informations-Service. (Hrsg.). (2019c). Foto des Monats. http://www.tis-gdv.de/tis/foto/2009/2009_07.htm. Zugriffem am 16.08.2019.
- Transport-Informations-Service. (Hrsg.). (2019d). Klima im Container. <http://www.tis-gdv.de/tis/containe/klima/klima.htm>. Zugriffem am 04.06.2019.
- Transport-Informations-Service. (Hrsg.). (2019e). Markierung von Packstücken. <http://www.tis-gdv.de/tis/verpack/markier/markier.htm>. Zugriffem am 08.06.2019.
- Transport-Informations-Service. (Hrsg.). (2019f). Teilverpackungen, Verschläge. <http://www.tis-gdv.de/tis/verpack/holz/packmitt/teilverp/teilverp.htm>. Zugriffem am 08.06.2019.
- Verbraucherzentrale. (2019). Internet-Bezahlssysteme. <https://www.verbraucherzentrale.de/wissen/digitale-welt/onlinehandel/welche-zahlungsmethoden-im-internet-sind-sicher-was-duerfen-sie-kosten-8368>. Zugriffem am 08.08.2019.
- Witte, H. (2000). *Allgemeine Betriebswirtschaftslehre*. München/Wien: R. Oldenbourg.

Reiner Siebert, geboren am 22. November 1956, ist seit dem 1. Februar 2019 Mitglied der Geschäftsleitung des GVNW. Nach einem Studium im Maschinenbau war Reiner Siebert von 1980 bis 1984 zunächst als Projektingenieur in der Industrie tätig, bevor er zum amerikanischen Industriever sicherer Factory Mutual wechselte. In der Zeit von 1984 bis 1993 war er dort unter anderem Account

Executive in Frankfurt sowie Underwriting Officer und Account Executive in London. 1993 wurde er Risk Manager UK & Ireland bei Akzo Nobel. Im Jahr 1997 übernahm Reiner Siebert die Position des Head of Risk Management bei der Virgin Travel Group in London. Dieses Amt hatte er bis Juli 2006 inne, bevor er im November 2006 zur Delvag Gruppe nach Köln wechselte und mit Wirkung vom 1. November 2007 zum Mitglied des Vorstands und der Geschäftsleitung der Albatros Versicherungsdienste GmbH ernannt wurde. Diese Rollen hielt er inne bis zum Eintritt in den einstweiligen Ruhestand Ende Oktober 2018.

Lukas Spohr absolvierte im Rahmen des „Kölner Modells“ das duale Studium im Fach Versicherungswesen mit den Schwerpunkten: Versicherungsvermittlung, Sachversicherung und Rückversicherung am Institut für Versicherungswesen der Technischen Hochschule Köln. Die zum dualen Studium zugehörige Ausbildung fand bei der Gothaer Finanzholding AG statt. Im Anschluss an das duale Studium studierte er, ebenfalls am IVW Köln, Risk & Insurance (M.Sc.). Zeitgleich arbeitete er als Werksstudent bei der Carl-Jaspers Versicherungskontor GmbH.



Terror- und politische Risiken

29

Leo Zagel, Volker Steinmetz und Hans Lange

Zusammenfassung

Industrieunternehmen haben sich insbesondere bei internationaler Geschäftstätigkeit, aber auch deutschlandweit mit verschiedensten Risiken zu befassen. Zu diesen Risiken gehört spätestens seit dem Vormittag des 11. Septembers 2001 und den Anschlägen auf das Word Trade Center in New York die Gefahr von Terroranschlägen. Neben diesen müssen sich die Unternehmen auch mit weiteren politischen Risiken auseinandersetzen, da sich die Strukturen von Land zu Land, aber auch von Region zu Region deutlich unterscheiden können und dies großen Einfluss auf den Erfolg der Unternehmung ausüben kann. Um diese Risiken im Rahmen des Risikomanagementprozesses zu managen, müssen zunächst die möglichen Risiken identifiziert und bewertet werden. Hierbei kommt es auch auf die Ursachen für Terror- und politische Risiken an. Je Risiko ist zu bewerten, ob es sich um ein vermeidbares Risiko handelt, ob das Risiko vermindert werden kann oder ob es im Rahmen einer entsprechenden Versicherung transferiert werden kann und sollte.

L. Zagel (✉) · V. Steinmetz

EXTREMUS Versicherungs-AG, Köln, Deutschland

E-Mail: leo.zagel@extremus.de; volker.steinmetz@extremus.de

H. Lange

TH Köln, Institut für Versicherungswesen, Köln, Deutschland

E-Mail: hans_lange@gmx.net

29.1 Einleitung

Für Industrieunternehmen gibt es viele Faktoren, die die Standortwahl, sowohl im Inland als auch im Ausland, beeinflussen können. Zwei dieser Faktoren sind zum einen die politische und soziale Stabilität und zum anderen das Terrorrisiko am möglichen Standort. Beide Faktoren spielen nicht nur bei ausländischen Direktinvestitionen, sondern auch bei der Unternehmensgründung und Standortwahl in Deutschland eine entscheidende Rolle.

Weltweit nimmt sowohl das politische Risiko, aber auch das Terrorrisiko in den letzten Jahren zu. Vergleichsweise stark sind diese Veränderungen in Entwicklungs- und Schwellenländern zu erkennen (vgl. Aon 2019).

Dass es weltweit derzeit zu politischen Verschiebungen und Risiken kommt, ist im Besonderen zu erkennen, seit Donald Trump zum Präsidenten der Vereinigten Staaten von Amerika gewählt worden ist. So zeigt sich, dass sich diplomatische Beziehungen rasant, teilweise durch einen einzelnen Tweet hervorgerufen, ändern können. Trump trifft sich einerseits mit seit Jahren schwierigen Verhandlungspartnern, wie zum Beispiel mit Kim Jong Un, dem Herrscher des nordkoreanischen Staates, welcher seit Jahren mit der Erforschung und dem Einsatz von Atomwaffen droht. Andererseits aber auch mit Wladimir Putin, dem russischen Präsidenten, welcher durch die Annexion der ukrainischen Halbinsel Krim gegen internationales Recht verstoßen hat. Weiterhin werden seit Jahren verhandelte Freihandelsabkommen durch Zölle gegenüber der EU oder der Volksrepublik Chinaersetzt.

Richtet man den Blick auf kleinere Mächte der Welt, so sind insbesondere Regionen des Nahen und Mittleren Ostens als unsicher zu identifizieren. Zahlreiche Regierungswechsel und Putschversuche sowie eine populistische Politik gehören vielerorts in den letzten Jahren zur Tagesordnung.

Diese Beispiele zeigen, dass die politische Situation und damit auch die politischen Risiken derzeit schwierig sind und die Investitionspolitik der Unternehmen beeinflussen kann.

Wie bereits vorab erwähnt, ist neben dem politischen Risiko aber auch das Terrorismusrisiko vermehrt zu beachten: Seit dem Vormittag des 11. September, als die Anschläge auf das World Trade Center in New York und das Pentagon in Washington D.C die Welt erschütterten, hat sich für die Versicherungswirtschaft im Hinblick auf Terrordeckungen einiges geändert. Erst- und Rückversicherer waren gezwungen, ihre Underwritingpolitik und somit die Versicherbarkeit des Terrorrisikos zu überdenken und anzupassen, um die Belastungen der Versicherungswirtschaft einzuschränken.

Auch in den folgenden Jahren gab es zahlreiche Terrorakte, die weltweit für Angst und Schrecken sorgten. Tab. 29.1 sind einige Beispiele der letzten Jahre zu entnehmen.

Dies zeigt, dass auch das Terrorismusrisiko ein weltweites Problem ist und nicht nur in Entwicklungs- und Schwellenländern auftritt, sondern auch in voll industrialisierten Ländern der „ersten Welt“.

Tab. 29.1 Internationale Terrorakte. (Quelle: GTD 2018; Spiegel 2019)

Datum	Ort	Anzahl Todesopfer	Anzahl Verletzte
26. November 2008	Mumbai, Taj Mahal Hotel	151	230
07. Januar 2015	Paris, Charlie Hebdo	12	12
26. Juni 2015	Tunesien, Hotelanlagen	40	36
13. November 2015	Paris, Bataclan	130	683
22. März 2016	Brüssel, Flughafen & Metrostation	35	270
14. Juli 2016	Nizza, Promenade	87	433
22. Mai 2017	Manchester, Arena	23	119
31. Mai 2017	Kabul, Nahe der deutschen Botschaft	93	491
03. Juni 2017	London, London Bridge	11	48
17. August 2017	Barcelona, Boulevard La Rambla	14	101
14. Oktober 2017	Mogadishu	588	316
21. April 2019	Sri Lanka	253	485

Tab. 29.2 Terrorakte in Deutschland. (Quelle: GTD 2018)

Datum	Ort	Anzahl Todesopfer	Anzahl Verletzte
05. September 1972	München, Olympiastadion	16	
1972–1993	RAF-Anschläge	>30	
26. September 1980	München, Oktoberfest	13	215
31. Juli 2006	Köln, Regionalzüge	Versuch	
04. September 2007	Oberschledorn, Sauerlandgruppe	Verhaftung	
02. März 2011	Frankfurt, Flughafen	2	2
18. Juli 2016	Würzburg, Regionalzug		5
22. Juli 2016	München, Einkaufszentrum	10	27
24. Juli 2016	Ansbach, Festival	1	15
19. Dezember 2016	Berlin, Breitscheidplatz	12	48
11. März 2017	Essen, Limbecker Platz	Terrorwarnung	
11. April 2017	Dortmund, BVB-Mannschaftsbus		1
10. Juni 2017	Köln, Flughafen	Terrorverdacht	
28. Juli 2017	Hamburg, Einkaufszentrum	1	7
07. Oktober 2018	Nürnberg, ICE	Versuch	

Dass auch Deutschland von Terroranschlägen nicht verschont geblieben ist, zeigt Tab. 29.2.

All diese Beispiele auf Seite der politischen Risiken, aber auch der Terrorrisiken, zeigen wie schwierig die jeweiligen Risiken derzeit für Unternehmen einzuschätzen sind. Dieses Kapitel soll sich daher damit befassen, wie sich politische- und Terrorrisiken erkennen und messen lassen. Weiterhin werden Möglichkeiten des Risikomanagements in Form von Risikovermeidung, -Verminderung und -Transfer dargelegt.

29.2 Grundlagen

Im Rahmen des nachfolgenden Kapitels wird das Risikomanagement von Terror- und politischen Risiken behandelt. Zunächst sind hierzu die grundlegenden Begriffe zu definieren.

29.2.1 Definition Terrorrisiko

Wie vorab erwähnt, spielt das Terrorrisiko für Unternehmen eine entscheidende Rolle. Für Terrorismus sowie dem Begriff des Terrorakts gibt es weltweit keine einheitliche Definition. Dies liegt insbesondere daran, dass der Begriff Terror im allgemeinen Sprachgebrauch für unterschiedliche und voneinander verschiedene Ereignisse benutzt wird. Bisher ist es noch nicht gelungen, eine einheitliche Definition, die für alle Länder gilt, zu finden.

Grund hierfür ist, dass der Terrorbegriff meist durch subjektive und moralische Sichtweisen nicht einheitlich betrachtet wird (vgl. Schneider et al. 2008, S. 17). Oftmals ist es noch nicht mal für verschiedene politische Institutionen innerhalb eines Landes gelungen, eine gemeinsame Begriffsdefinition zu finden und zu benutzen. Als Beispiel seien hier einige Begriffsdefinition von US-amerikanischen Behörden genannt. So lautet die Definition der Central Intelligence Agency (CIA) wie folgt:

- „Terrorismus ist vorsätzliche, politische motivierte Gewalt, verübt gegen zivile Ziele durch substaatliche Gruppen oder im Verborgenen arbeitende Täter. Gewöhnlich mit der Absicht ein Publikum zu beeinflussen.“ (CIA 2010)

Das Federal Bureau of Investigation (FBI) hingegen geht von folgender Definition aus:

- „Terrorismus ist die rechtwidrige Anwendung von Gewalt gegen Personen oder deren Eigentum, um eine Regierung, die Zivilbevölkerung oder einen Teil davon einzuschüchtern oder zu etwas zu zwingen. Absicht dieser Gewaltanwendung ist es politische oder soziale Ziele zu erreichen.“ (FBI 2019).

Dies zeigt, wie schwierig eine einheitliche Begriffsbestimmung ist.

Die wohl in Deutschland anerkannteste Definition ist den ATB 2016 zu entnehmen, in denen die Terrorakte wie folgt definiert werden:

- „Terrorakte sind jegliche Handlungen von Personen oder Personengruppen zur Erreichung politischer, religiöser, ethnischer oder ideologischer Ziele, die geeignet sind Angst und oder Schrecken in der Bevölkerung oder Teilen der Bevölkerung zu verbreiten und dadurch auf eine Regierung oder staatliche Einrichtungen Einfluss zu nehmen.“

Die ATB grenzen im weiteren Verlauf das Terrorrisiko insbesondere durch Ausschlüsse von Ereignissen wie (Bürger-)Krieg, Revolutionen, Rebellionen oder Aufständen ab. Weiterhin gelten auch Plünderungen oder Verfügungen von Hoher Hand im Sinne der ATB nicht als Terrorakte.

Im weiteren Verlauf des Buchkapitels wird bei dem Terrorbegriff von obiger Definition gemäß der ATB ausgegangen.

Im Allgemeinen wird davon ausgegangen, dass der Begriff aus der Zeit der französischen Revolution stammt, als 1793/1794 durch das sogenannte „Regime de la terreur“ der revolutionäre Terrorismus ausgerufen wurde (vgl. Schneider et al. 2008, S. 17). Zu dieser Zeit galt Terrorismus noch als Tugend, mit deren Hilfe ein korruptes System zu zerstören und so die Demokratie zu erlangen sei.

Heute wird der Begriff seitens der Staatsgewalt stets mit etwas Negativem assoziiert, Terroristen selbst bezeichnen sich als Helden oder Befreier. Oftmals wird davon ausgegangen, dass es Ziel des Terrorismus ist, sowohl Angst zu verbreiten als auch maximale Aufmerksamkeit zu erreichen (vgl. Schneider et al. 2008, S. 17). Dies wird insbesondere durch hohe Opferzahlen und damit einhergehendem medialen Interesse erreicht.

29.2.2 Definition politisches Risiko

Für die Entscheidungsfindung eines Unternehmens in ein Land zu investieren bzw. zur Ermittlung des Risikos der Unternehmung, wenn bereits ein Beteiligungsverhältnis mit einem Unternehmen in einem Land oder ein Tochterunternehmen in dem Land vorliegt, spielt insbesondere die politische Situation eine wichtige Rolle.

Historisch taucht der Begriff des politischen Risikos in der Literatur erst in den 1970er-/1980er-Jahren auf. Zu dieser Zeit stiegen die ausländischen Direktinvestitionen in Entwicklungsländer stark an. Dies führte dazu, dass zum ersten Mal das Risikoempfinden hinsichtlich dieser Risikomöglichkeiten anstieg. Beispiele für erste entsprechende Ereignisse sind der Ölpreisschock Mitte der 1970er-Jahre sowie die islamische oder auch iranische Revolution von 1979, bei der nach dem Sturz der Schah-Regierung durch die Revolutionäre unter der Führung von Ayatollah Ruhollah Chomeini die Islamische Republik Iran gegründet wurde. Viele Iraner machten vor allem die USA für die prowestliche Politik und die Unterdrückung durch den Schah verantwortlich (vgl. Naini 1979, S. 15 ff.). In der Folge kam es zu einer politischen Änderung und zahlreiche Verträge und Vereinbarungen wurden gegenüber den ausländischen Unternehmen nicht mehr eingehalten.

Die derzeit anerkannteste Definition in der Literatur geht auf Howell zurück (vgl. Howell 2001). Er bezieht den Begriff des „politischen Risikos“ auf die Möglichkeit, dass politische Entscheidungen in einem Land das Investitionsklima in der Art beeinflussen, dass Investoren Ihr Geld verlieren beziehungsweise der erwartete Gewinn verringert wird. Seine Definition umfasst neben den politischen Entscheidungen auch politische und gesellschaftliche Ereignisse, wie zum Beispiel Revolten und Aufstände. Als mögliche politische Risiken beschreibt Howell die folgenden acht Unterpunkte:

- Unconvertibility – Währungssinkonvertibilität,
- Expropriation or Nationalization – Enteignung oder Verstaatlichung,
- Civil Strife Damage – Bürgerkriegsschäden,
- War Damage – Kriegsschäden,
- Contract Repudiation – Vertragsbruch,

- Negative Government Actions – Negative Regierungsaktionen,
- Losses from Process Deterioration – Prozessverschlechterungen,
- Losses from event intervention – Verhinderung/Eingriff in die Unternehmung.

Im weiteren Verlauf dieses Kapitels wird für politische Risiken diese Definition von Howell angenommen.

29.3 Ursachen

Sowohl Terror, als auch politischen Risiken werden durch Verhaltensweisen der Menschen beeinflusst und so hervorgerufen. Dieses Verhalten ist nicht auf Grundlage mathematischer Formeln vorherzusehen. Um jedoch die Risiken zu erklären und im weiteren Verlauf zu identifizieren und zu bewerten, ist zunächst zu schauen, welche Ursachen für die entsprechenden Risiken verantwortlich sein können.

29.3.1 Ursachen von Terrorrisiken

Die Motive zur Entstehung von Terrorismus bzw. für die Gründung terroristischer Einheiten sind unterschiedlicher Natur. Um diese Gründe besser zu verstehen, muss zunächst zwischen nationalem, internationalem und transnationalem Terrorismus unterschieden werden. Nationale Terrorgruppierungen, wie zum Beispiel die ETA in Spanien oder die IRA in Irland, konzentrierten sich auf Angriffsziele im Staatsgebiet, wohingegen internationale Terrorgruppierungen Bewohner unbeteigter Staaten als Angriffsziele für sich ausgemacht haben (vgl. Schneider et al. 2008, S. 35). Ziel von transnationalem Terrorismus ist es hingegen, jeweils die derzeitige internationale Ordnung im Sinne der eigenen Ideologien zu verändern (vgl. Schneider et al. 2008, S. 36).

An dieser Einordnung lässt sich erkennen, dass je nach Ziel die Ursachen des Terrorismus abweichend sind. Eine mögliche Ursache ist die Außenpolitik eines Landes. Hierbei wird der Terrorismus als Instrument der Staatspolitik im Sinne der Regierung missbraucht. Staatlich gefördert ist es so möglich, durch Gewalt gegenüber der Zivilbevölkerung politische Ziele zu erreichen.

Neben den staatlichen Motiven wird auch immer wieder von Terrorismus aus religiösen Motiven gesprochen. Hierunter zu verstehen sind religiöse Schriften und Lehrmeinungen, aus der eine von Gott gegebene Pflicht resultiert, Gewalt auszuüben.

Eine weitere Ursache wird in der Literatur in der sozialen Ungleichheit und Unterdrückung gesehen. Die Betroffenen versuchen, ihrer Situation zu entfliehen. Es kommt zu Konflikten in der Gesellschaft, die oftmals mit politischer Gewalt und gezieltem Terrorismus bekämpft werden sollen (vgl. Schneider et al. 2008, S. 47).

29.3.2 Ursachen politischer Risiken

Welche Ursache genau für die Entstehung eines bestimmten Risikos verantwortlich ist, ist nicht immer zu erkennen. Die Ursache kann sowohl im betroffenen Land selbst verankert, aber auch mit der Unternehmung begründet sein.

Zahlreiche politische Risiken hängen eng mit der politischen und sozialen Struktur im betroffenen Land zusammen. So können Sitten, Gebräuche, religiöse Ansichten sowie Wertvorstellungen zwischen dem Investor und der Gesellschaft im jeweiligen Land stark variieren. Denkbar sind hier auch daraus resultierende Risiken. Nach Balleis sind besonders ethnologisch-linguistische und demografische Strukturen langfristig unveränderbar (vgl. Ballais 1985, S. 101). Besonders in Entwicklungsländern kommt es immer wieder zu Auseinandersetzungen zwischen unterdrückten Minderheiten und den dazugehörigen, meist herrschenden Mehrheiten. Diese Auseinandersetzungen können teilweise bewaffnet sein und zu bürgerkriegsähnlichen Situationen vor Ort führen. Solche Situationen können natürlich Investoren abschrecken. Ein von den Industrieländern bzw. ehemaligen Kolonialnationen selbst geschaffenes Problem war und ist noch immer die Grenzziehung auf dem afrikanischen Kontinent. Noch heute gibt es Gruppierungen über Landesgrenzen hinweg, die nach Unabhängigkeit streben. Auch hier kommt es regelmäßig zu Aufständen und bewaffneten Kämpfen.

Ein weiterer Risikofaktor ist die steigende Bevölkerung in den Entwicklungsländern. Ist das Bevölkerungswachstum deutlich größer als das Wirtschaftswachstum, so kann von einer Überbevölkerung gesprochen werden. Eine Überbevölkerung kann die Verbreitung von Wohlstand verhindern (vgl. Ballais 1985, S. 102). Mögliche Folgen aus der demografischen Entwicklung sind in der Regel Arbeitslosigkeit und soziale bzw. wirtschaftliche Ungleichheit zwischen verschiedenen Schichten in der Gesellschaft des Landes. Das heißt, die Schere zwischen Arm und Reich driftet auseinander. Diese Veränderungen kräftigen das Konfliktpotenzial zwischen den verschiedenen Schichten und führen so unmittelbar zu einem politischen Risikofaktor.

Kommt es nun zu Investitionen in einem Land, bei dem nur ein Teil der dort lebenden Gesellschaft profitiert, sind steigende Spannungen aufgrund des Wohlstandsgefälles die Folge (vgl. Alderson 2003, S. 323 ff.). Es ist schwierig, für Regierungen vorbeugende Maßnahmen zu treffen, ohne Investoren soweit einzuschränken, dass diese die Investition lieber anderweitig tätigen, als im entsprechenden Land.

Ein weiteres Risikopotenzial stellt die Struktur des Staates und in erster Linie der Regierung da. Eine geschwächte oder unfähige Regierung neben einer starken und wachsenden Opposition, egal ob parlamentarisch oder außerparlamentarisch, kann zu weiteren Unruhen im Investitionsland führen. Diese Unruhen können zwar mithilfe des Militärs unterdrückt werden. Eine militärgestärkte Regierung besitzt in der Regel jedoch nur geringen Rückhalt in der Bevölkerung. Dass hieraus neue weitere Risiken entstehen können, ist offensichtlich. Gerade weil das Militär in diesem Fall bestimmen kann, wie die Regierung aussieht, kann es kurzfristig zu Veränderungen in der Zusammensetzung der Regierung

und dadurch auch in der Wirtschaftspolitik geben (vgl. Ballais 1985, S. 107). Die Regierungen können außerdem begrenzen, welche Unternehmen beziehungsweise welche Branchen in ihrem Land tätig werden dürfen. Besonders Branchen, die strategisch für die Regierung wichtig sind, werden nur selten von ausländischen Direktinvestoren eingenommen. Die Regierungen, insbesondere das jeweilige Militär, möchten in ihrer Struktur nicht beeinflusst werden und lassen dies oftmals auch nicht zu.

Treffen multinationale Unternehmen mit ihren ausländischen Direktinvestitionen dort auf besondere Wertvorstellungen, kommt es häufig zu Konfliktpotenzial. Dies stellt somit ein weiteres politisches Risiko dar. Besonders nationalistische Regierungen lassen keine Investitionen zu, aus denen hauptsächlich ausländische Privatpersonen oder Investoren Gewinne generieren. Versucht eine nationalistisch geprägte Regierung, die Gewinne im Land und bei der eigenen Bevölkerung zu behalten, steigt auch das Risiko der Enteignung (vgl. Ballais 1985, S. 109 f.).

Neben den jeweiligen Regierungen kann auch die Bevölkerung selbst ein Risikopotenzial darstellen. Friedliche Demonstrationen sind meist nur ein frühzeitiger Hinweis auf entstehende politische Konflikte. Steigen in Folge dessen die Spannungen, kann es zu Unruhen oder gar Revolten kommen, bei denen auch Gewalt angewendet wird. Diese stellen ebenfalls eine Gefahr für das Eigentum und die Sicherheit der Investition dar (vgl. Ballais 1985, S. 113).

Politische Aufrühere sind jedoch nicht nur Risiken für Entwicklungsländer. Auch in Industrieländern kommt es regelmäßig zu Demonstrationen. Dass diese auch mit Gewalt verbunden sein können, zeigte zum Beispiel der G20-Gipfel in Hamburg im Jahr 2018 (vgl. Zajak et al. 2018).

Neben diesen internen Faktoren im jeweiligen Land spielen für politische Risiken auch externe Faktoren eine entscheidende Rolle. Zum einen seien hier Sanktionen genannt, die auch ausländische Direktinvestitionen treffen können. Gibt es zum Beispiel ein internationales Handelsembargo, so kann es für hiervon im jeweiligen Land betroffene multinationale Unternehmen vor Ort schwierig werden, Rohstoffe zu erhalten bzw. fertige Endprodukte außerhalb des Landes zu verkaufen. Aber auch die Möglichkeit der Enteignung bei Spannungen zwischen zwei Ländern spielt eine wichtige Rolle bei der Ermittlung möglicher Risiken. Gibt es politische Spannungen zwischen zwei Ländern, so kann zum Beispiel ein Land ein Unternehmen allein aus dem politischen Grund enteignen, hierüber Macht gegenüber dem anderen Land auszuüben (vgl. Ballais 1985, S. 122). Wie lange eine erfolgreiche Zusammenarbeit mit dem Unternehmen selbst stattgefunden hat, spielt hierbei meist keine Rolle. Dies zeigt auch, dass sowohl Entwicklungsländer als auch Industriestaaten von politischen Risiken betroffen sein können.

29.4 Risikoidentifizierung und Risikobewertung

Zur Messung und Bewertung der Terror- und politischen Risiken wurden im Laufe der Jahre verschiedenste qualitative und quantitative Methoden entwickelt. Hiermit solle den Industrieunternehmen insbesondere im Rahmen des Risikomanagements Unterstützung in

der Entscheidungsfindung gegeben werden. Im Folgenden werden einige Modelle zur Risikoidentifizierung und Risikobewertung vorgestellt.

29.4.1 Terrorrisiken

Im Anschluss an die Terroranschläge des 11. September 2001 wurde insbesondere den Versicherern bewusst, dass hierdurch finanzielle Schäden in Höhen entstehen können, von denen bisher nicht ausgegangen werden konnte. Um den maximalen Höchstschatzen und den dazugehörigen Einfluss auf das Unternehmen zu messen, stehen den Versicherern sowie den zu versichernden Unternehmen quantitative und qualitative Methoden zur Verfügung.

Zunächst wird für die quantitative Methode der maximale Höchstschatzen oder auch „Probable Maximum Loss“ (PML) für das jeweilige zu versichernde Unternehmen ermittelt. Im Verständnis der Versicherer ist der PML der geschätzte wahrscheinlich höchste Schaden, mit dem durch ein einzelnes Ereignis unter Berücksichtigung der Risikogegebenheiten bei vorsichtiger Betrachtung gerechnet werden muss. Hierbei wird von zufälligen Schadenereignissen ausgegangen, denen jedoch bereits schadenmindernde Maßnahmen hinzugerechnet werden. Üblicherweise werden die PML der Feuerversicherung und der Betriebsunterbrechungsversicherung zur Ermittlung des maximalen Höchstschatzens zusammengerechnet. Wie hoch die Auswirkung eines maximalen Höchstschatzens für das Unternehmen sein kann, wird erst durch Betrachtung des Verhältnisses von PML zum Eigenkapital möglich (vgl. Pabst 2008, S. 77 f.).

Neben der Analyse quantitativer Merkmale spielen auch verschiedene qualitative Merkmale eine entscheidende Rolle bei der Risikomessung und Risikobewertung von Terrorrisiken. Hierbei werden zum einen regionale Merkmale, aber auch weitere risikoerhöhende Kriterien betrachtet. Die Ermittlung der regionalen Risikosituation kann durch verschiedene Faktoren ermittelt werden. Hier kann es insbesondere relevant sein, ob sich das zu versichernde Unternehmen bzw. Gebäude in einem Ballungsgebiet befindet. Die Extremus Versicherungs AG teilt im Tarif 2008 Deutschland in insgesamt drei Regionalklassen ein:

In Region I befinden sich die Stadtkerne der Städte mit mehr als 500.000 Einwohner sowie Großflughäfen mit einem Fluggastaufkommen von mehr als fünf Millionen Passagieren pro Jahr. In dieser Region befinden sich derzeit die Stadtzentren von 15 Großstädten und acht Flughäfen.

In Region II befinden sich die restlichen Stadtgebiete der Großstädte sowie alle deutschen Großstädte mit mehr als 100.000 Einwohnern.

Alle übrigen Regionen werden der Risikoklasse III zugeordnet.

Weitere qualitative Risikomerkmale können mit der Spezifikation des zu versichernden Gebäudes zusammenhängen. Hier ist zum Beispiel relevant, ob das Objekt selbst als Stattssymbol gilt oder ob das Objekt selbst spektakuläre Terrorschäden auslösen kann.

So geht der Extremus Tarif 2008 von folgenden risikoerhöhenden Spezifikationen für Gebäude und Unternehmen aus:

1. Flughäfen, Bahnhöfe,
2. symbolhafte Gebäude, Wahrzeichen und Gebäude mit politischer Bedeutung,
3. Sportstadien und Veranstaltungshäuser mit Fassungsvermögen von mehr als 10.000 Personen sowie Messehallen,
4. Rundfunk- und TV-Sender, Zeitungsverlage und Rechenzentren,
5. Tunnel, Brücken und Staudämme,
6. Kraftwerke, Wasserwerke und Funktürme,
7. Gebäude mit mehr als 20 Etagen,
8. Chemie und Wehrtechnik.

Hilfe bei der Risikokalkulation bieten auch verschiedene Bewertungsmodelle, die im Anschluss an die Anschläge vom 11. September 2001 entwickelt wurden. Die Genauigkeit dieser Modelle ist bisher jedoch kaum zu quantifizieren, da sie der Realität bis dato noch nicht standhalten mussten. Trotz häufiger Kritik an solchen Modellen, unter anderem dass sich menschliches Verhalten und die damit verbundenen Wahrscheinlichkeiten für Terroraktivitäten gar nicht oder nur kaum messen ließen, sei an dieser Stelle das Bewertungsmodell des amerikanischen Unternehmens RMS kurz vorgestellt.

Dieses Modell wird auch als probabilistisches Terrorismusmodell bezeichnet, das heißt, dass in diesem Modell auch entsprechende Wahrscheinlichkeiten Einfluss nehmen. Es betrachtet die folgenden Komponenten (vgl. RMS 2014):

- Die potenziellen Ziele sowie die möglichen Angriffsmodi:
- Hier wird zunächst danach unterschieden, wo sich das potenzielle Ziel befindet. So sind Ziele in Großstädten gefährdet als Ziele in ländlichen Regionen. Darüber hinaus ist nicht jedes Ziel für sämtliche Arten von Angriffsmodi gleich anfällig. Hierbei werden sowohl konventionelle als auch CBRN- (chemisch-biologisch, radiologisch und nuklear) Angriffsmöglichkeiten berücksichtigt.
- Die relative Wahrscheinlichkeit eines Angriffs:
- Auch hierbei werden das Ziel und die Art des Angriffs berücksichtigt. So sind Angriffe mit konventionellen Bomben wahrscheinlicher und leichter zu planen als Angriffe mit chemischen Waffen. An dieser Stelle wird darüber hinaus bewertet, um welche Art von Ziel es sich handelt. Orte mit hoher symbolischer oder wirtschaftlicher Bedeutung sind wahrscheinlichere Angriffsziele.
- Die relative Wahrscheinlichkeit, dass mehrere Angriffe ein einzelnes Ereignis bilden:
- In der Vergangenheit zeichneten sich viele Terroranschläge dadurch, dass zwei oder mehr Ziele gleichzeitig angegriffen wurden.
- Ereignishäufigkeit:
- Diese wird anhand von empirischen Daten ermittelt und durch insgesamt drei Parameter bestimmt. Diese sind die Anzahl der versuchten Ereignisse in einem Jahr, die Er-

folgsrate der versuchten Anschläge sowie ein Unterdrückungsfaktor, der auf die Reaktion der Regierung im Anschluss an einen Anschlag basiert (vgl. hierzu RMS 2014).

Trotz der verschiedensten Bewertungsmodelle ist es nicht möglich, zukünftige Terroranschläge betreffend Häufigkeit, Ort und Härte voraus zu sagen (vgl. Pabst 2008, S. 81). Dies liegt insbesondere daran, dass das Verhalten der Terroristen kaum in mathematischen Formeln dargestellt werden kann (vgl. Surminski 2003, S. 222).

Für die gesamte Risikomessung des Terrorrisikos müssen sowohl die qualitativen als auch quantitativen Merkmale betrachtet werden. Erst im Anschluss daran kann für jedes Unternehmen individuell entschieden werden, ob die Absicherung des Terrorrisikos als sinnvoll erscheint. Auf die verschiedenen Formen der Absicherungsmöglichkeiten wird im späteren Verlauf dieses Kapitels eingegangen.

29.4.2 Politische Risiken

Zur Messung und Bewertung länderspezifischer politischer Risiken wurden im Laufe der Jahre viele Methoden entwickelt. Diese können ebenfalls sowohl quantitativ als auch qualitativ sein. Einfacher und daher auch kostengünstiger sind hierbei die qualitativen Methoden. Hierbei wird in der Regel auf Expertenmeinungen vertraut. Quantitative Methoden hingegen versuchen, statistische Daten, Quoten und Ratings mit fundierten Expertenmeinungen zu verbinden.

Im Folgenden werden die gängigsten Methoden zur Risikomessung und -Bewertung von politischen Risiken dargestellt.

Die wohl am häufigsten angewandten qualitativen Methoden sind Umweltanalysen, Prüflistverfahren und Expertenbefragungen.

Bei der Umweltanalyse wird im Zuge der Überlegungen, an welchem Standort eine ausländische Direktinvestition am sinnvollsten ist, ein einzelner Manager oder ein ganzes Team in das jeweilige in Frage kommende Gebiet entsandt. Diese Expertengruppe trifft sich direkt vor Ort mit Regierungsorganisationen, Mitgliedern verschiedener Wirtschaftsverbände sowie anderen bereits vor Ort ansässigen Unternehmen. Im Anschluss an die Reise in das Gebiet wird dann über die besonderen Gegebenheiten an die Geschäftsführung berichtet, was bei der weiteren Entscheidungsfindung einen wichtigen Einfluss haben kann.

Im Prüflistverfahren wird versucht, anhand von Checklisten die politische Situation in den jeweiligen in Frage kommenden Gebieten und Ländern darzustellen. Hierbei ist es wichtig, durch konkrete Fragen und Faktoren die Prüfliste möglichst genau zu gestalten. Weiterhin ist es bei dieser Methode besonders wichtig, auf sowohl interne als auch externe Aspekte einzugehen (vgl. Haan 1984).

Interne Aspekte der Länder können hierbei zum Beispiel die Historie, die Regierung oder die Homogenität der Gesellschaft sein, wohingegen externe Aspekte die Kriegsgefahr in der Region sowie die geltenden Wirtschaftsbeziehungen sind. Ein wichtiger Vorteil

dieser Methode ist, dass für jedes Unternehmen individuelle Prüflisten erstellt werden können und so auf alle relevanten Parameter eingegangen werden kann.

Eine dritte qualitative Methode ist die Einholung von Expertenmeinungen. Je nach Unternehmen können hier Unternehmensberater, Wirtschaftsexperten, Politiker oder Politikwissenschaftler die richtigen Ansprechpartner sein. Auch der von der GTAI (Germany Trade and Invest) als Nachfolger der Bundesagentur für Außenwirtschaft herausgegebene Länderbericht kann hierbei herangezogen werden. Da bei dieser Methode keine Gespräche vor Ort geführt werden, ist es sinnvoll, die verschiedenen Methoden zu kombinieren.

Darüber hinaus gibt es auch quantitative Methoden zur Erfassung politischer Risiken. Diese sind deutlich aufwendiger, da hierfür zunächst statistisches Datenmaterial erstellt werden muss, welches im weiteren Verlauf mit differenzierten Expertenmeinungen ins Verhältnis gebracht werden muss. So lassen sich verschiedene Variablen erkennen und gewichten.

Im Folgen werden zwei gängige Methoden zur Ermittlung der politischen Risiken vorgestellt:

Der international Country Risk Guide (ICRG) der PRS Group vergleicht insgesamt 22 Variablen in den drei Kategorien politisches Risiko (PR), ökonomisches Risiko (ER) und finanzielles Risiko (FR). Das politische Risiko wird hierbei doppelt gewichtet. Dies zeigt, wie wichtig politische Risiken für Erfolg oder Misserfolg einer ausländischen Direktinvestition sein können.

In Tab. 29.3 werden die verschiedenen Kategorien, die für die Betrachtung der politischen Risiken herangezogen werden, dargestellt und gewichtet.

Ein Nachteil des ICRG der PRS-Group ist jedoch, dass nicht alle Bewertungen auf statistischen Zahlen beruhen, sondern auch Expertenmeinungen mit einbezogen werden, die teilweise subjektiv geprägt sein können. Auch sind die Risiken nicht für alle Unterneh-

Tab. 29.3 Kategorien für politische Risiken und deren Gewichtung nach der PRS-Group. (Quelle: PRS-Group 2018)

Risikokategorie	Gewichtung in %
Regierungsstabilität	12
Sozioökonomischer Druck	12
Investitionsrisiken (Enteignung, Gewinnrückführung, Zahlungsverzögerungen)	12
Interne Konflikte (Bürgerkriegsrisiko, Terror & politische Gewalt, Störung der öffentlichen Ordnung)	12
Externe Konflikte (Krieg, internationale Konflikte, Druck anderer Länder)	12
Korruption	6
Militärischer Einfluss in die Politik	6
Religiöse Spannungen	6
Rechtssystem und Ordnung (z. B. Kriminalitätsraten)	6
Ethnische Spannungen	6
Regierung (Spanne von Demokratie bis Autarkie)	6
Qualität der Bürokratie	4

Tab. 29.4 Kategorien für politische Risiken und deren Gewichtung nach BERI. (Quelle: BERI 2018; Köpplinger 1986, S. 79 ff.)

Risikokategorie	Gewichtung in %
Politische Stabilität	12
Einstellung gegenüber ausländischen Investoren und Gewinnen	6
Expropriation	6
Inflation	6
Zahlungsbilanz	6
Bürokratische Hemmnisse	4
Wirtschaftswachstum	10
Währungskonvertibilität	10
Durchsetzbarkeit von Verträgen	6
Lohnkosten/Produktivität	8
Verfügbarkeit örtlicher Fachleute und Lieferanten	2
Nachrichten/Transport	4
Ortsansässiges Management und Partner	4
Verfügbarkeit kurzfristiger Kredite	8
Verfügbarkeit langfristiger Kredite und Eigenkapital	8

men gleich zu gewichten. Je nach Branche und Absatzmodell sollten daher entsprechende Anpassungen vorgenommen werden.

Eine weitere quantitative Methode ist der Operation Risk Index von Beri (vgl. Tab. 29.4). Bei diesem Modell wird neben dem PRI (Political RIisk Index) auch der ORI (Operational Risk Index) gebildet und im Anschluss mit einem abschließenden R-Faktor, der die Zahlungsfähigkeit des jeweils betrachteten Landes wiedergibt, multipliziert. Im Rahmen des PRI werden hierbei 15 Faktoren betrachtet und gewichtet.

Das Besondere des Operation Risk Index ist, dass sowohl eine Vergangenheitsbetrachtung, eine Gegenwartsbetrachtung sowie ein Blick in die Zukunft möglich ist. Dieser Ausblick beträgt entweder ein Jahr oder bis zu fünf Jahren.

Beide Modelle liefern Ergebnisse für fast alle Länder, sodass entsprechende Ranglisten erstellt werden können und so ein Vergleich zwischen verschiedenen Standorten möglich ist.

29.5 Risikomanagement

Es stellt sich im Weiteren die Frage, ob das jeweilige Risiko vermeidbar ist oder ggf. gemindert werden kann. Hier können zum Beispiel Diversifizierungseffekte eine entscheidende Rolle spielen.

29.5.1 Vermeidung

Die einfachste und je nach den vorab erwähnten Länderratings und den daraus resultierenden Einstufungen sinnvollste Möglichkeit einer Risikovermeidung kann sein, auf eine geplante Investition zu verzichten. Politische Risiken treten somit erst gar nicht auf und auch das Terrorrisiko ist für das entsprechende Projekt nicht mehr vorhanden. Eine weitere Möglichkeit ist es, als Unternehmen nur in vergleichsweise sicheren Gebieten welt- aber auch deutschlandweit ansässig bzw. tätig zu sein. Dies sollte idealerweise auch für die entsprechenden Vertragspartner gelten.

Eine Möglichkeit zur Vermeidung verschiedener politischer Risiken kann es sein, mit diversen staatlichen Organisationen Verabredungen und Verträge einzugehen. Die Auswahl der Organisation(en) sollte sorgfältig getroffen werden (vgl. Brink 2016, S. 156 f.). Ein enges Verhältnis mit bestehenden Regimen birgt jedoch auch die Gefahr, dass bei einem politischen Wechsel genau diese Verträge nicht mehr gültig sind bzw. nicht mehr eingehalten werden (vgl. Versicherungspraxis 11/2016).

29.5.2 Verminderung

Eine offensichtliche und meist auch angewandte Methode zur Minderung von terroristischen Aktivitäten und Anschlägen auf ein Objekt des entsprechenden Unternehmens ist sicherlich die Personen- und Wareneingangskontrolle, sobald das Betriebsgrundstück betreten wird. Auch Reisesicherheitsmanagement und Sicherheitsschulungen für das Personal sind mögliche Methoden, um das Risiko und vor allem die im „Worst Case“ vorhandenen Auswirkungen zu minimieren (vgl. Versicherungspraxis 11/2016).

Eine weitere Möglichkeit zur Minimierung des Terrorrisikos, aber auch der vorab angesprochenen politischen Risiken, stellt die Erstellung von Notfallplänen und die Einführung eines Krisenstabs und eines Handbuchs zum Verhalten in Krisensituationen dar (vgl. Versicherungspraxis 11/2016). In Kombination dazu kann ein Frühwarnsystem stehen. Gewisse politische Aktivitäten weisen darauf hin, dass sich die Politik in eine für das Unternehmen negative Stimmung verschlechtern kann. Dies gilt zum Beispiel für Verfassungsänderungen, die einer Regierung diktatorische Rechte verleihen können. Ob die im Anschluss entstehenden negativen Auswirkungen für das Unternehmen nun von der Regierung selbst ausgehen oder aber durch von anderen Regierungen gesteuerte Sanktionen entstehen, spielt hierbei keine Rolle.

Eine weitere Methode der Risikominderung besteht darin, weltweit in verschiedene Länder zu investieren, was im Rahmen von Auslandsinvestitionen nicht immer möglich ist. Dies gilt insbesondere für Direktinvestitionen, die getätigt werden, um Zugang zu bestimmten Rohstoffen zu erhalten.

29.5.3 Risikotransfer

Sowohl für das Terrorismusrisiko als auch für politische Risiken gibt es Absicherungsmöglichkeiten für Unternehmen in Form entsprechender Versicherungslösungen.

Mit Blick auf das Terrorismusrisiko gibt es meist staatlich geförderte Pools, die zur Absicherung herangezogen werden können. Diese sind in der Regel jeweils nur auf das staatliche Territorium beschränkt (vgl. Thomann 2007). In Deutschland ist zum Beispiel eine Absicherung für die auf deutschem Gebiet befindlichen Objekte über die EXTREMUS AG möglich.

Da viele Unternehmen multinationale Geschäfte betreiben, ist in den jeweiligen Ländern das Terrorrisiko bei Bedarf über den entsprechenden, im Land bestehenden Terrorpool abzusichern. Tab. 29.5 sind einige dieser Terrorpools mit Sitz in der EU bzw. USA zu entnehmen, wobei an dieser Stelle darauf hingewiesen sei, dass es sich teilweise um Pflichtversicherungen handelt.

In Deutschland wurde die EXTREMUS AG am 03. September 2002 im Anschluss an die Anschläge auf das WTC am 11. September 2001 auf Initiative der deutschen Versicherungswirtschaft gegründet. An der Gründung waren neben dem Gesamtverband der deutschen Versicherungswirtschaft (GDV) auch die Bundesregierung und der Bundesverband der deutschen Industrie (BDI) beteiligt.

Dieses Terrorversicherungskonzept beinhaltet zwei Komponenten: Zum einen schließen Erstversicherer das Terrorrisiko in ihren Feuer-/BU-Versicherungen bis zu einer Gesamtversicherungssumme von 25 Millionen Euro nicht aus. Zum anderen deckt der Spezialversicherer EXTREMUS (vgl. Abb. 29.1) Terrorschäden bis zu einer Jahreshöchstentschädigung von neun Milliarden Euro für Risiken oberhalb von 25 Millionen Euro ab. EXTREMUS selbst trägt hiervon 2,52 Milliarden Euro. Für darüber hinaus gehende Entschädigungen steht eine Staatsgarantie von 6,48 Milliarden Euro zur Verfügung. Die maximale Jahreshöchstentschädigung beträgt jedoch maximal 1,5 Milliarden Euro pro Versicherungsnehmer/Industrieunternehmen.

Tab. 29.5 Terrorpools mit Sitz in der EU bzw. USA

Land	Name	Gründungsjahr
Deutschland	EXTREMUS AG	2002
Großbritannien	Pool RE	1993
Frankreich	GAREAT	2002
USA	TRIA/TRIPRA	2002/2008
Belgien	TRIP	2008
Österreich	VVO	2002
Schweiz	SVV Treaty Cover	2003

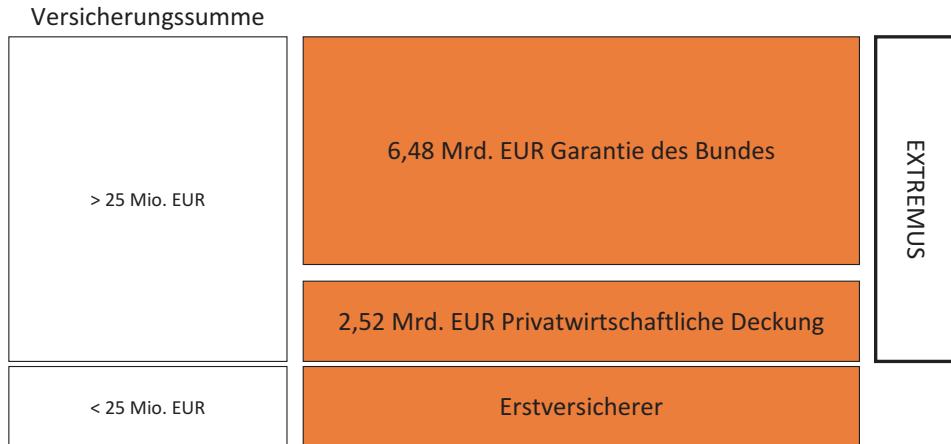


Abb. 29.1 Extremus AG. (Quelle: eigene Darstellung)

Für den Transfer von politischen Risiken bieten sich verschiedene Möglichkeiten. Auch diese sind zum Teil staatlich gefördert, jedoch werden auch von privatwirtschaftlichen Versicherern Absicherungsmöglichkeiten angeboten. So bietet zum Beispiel Euler Hermes Deutschland in ihrem Portfolio Exportkreditversicherungen für deutsche, aber auch für weltweit tätige Unternehmen an (vgl. Diekmann 2002, S. 28 ff.).

Eine weitere Möglichkeit zum Schutz ausländischer Direktinvestitionen gegen Enteignungen von Vermögenswerten, Unruhen, Krieg oder Währungsinkonvertibilitäten bieten multilaterale Organisationen an, wie zum Beispiel die Multilateral Investment Guarantee Agency (MIGA). Die MIGA wurde 1988 als Teil der Weltbankgruppe gegründet und besteht derzeit aus 181 Mitgliedern (vgl. Miga 2017, S. 16). Ziel ist es hierbei, zum einen Direktinvestitionen in weniger entwickelte Länder abzusichern, aber auch Investitionen in eben diese Länder zu fördern und in Form von Beratung zu unterstützen. Bei einer maximalen Laufzeit von 15 bis 20 Jahren liegt die Höchstversicherungssumme hierfür derzeit bei 250 Millionen US-Dollar. Darüber hinaus ist es nur möglich, sich dort gegen Risiken zu versichern, gegen die das Herkunftsland selbst keine anderen Schutzmaßnahmen getroffen hat, wie zum Beispiel durch bilaterale Schutzabkommen. Die MIGA kann daher nur als Ergänzung zu bereits vorhandenen Absicherungsmechanismen verstanden werden.

Selbstredend ist eine solche Absicherung bzw. ein solcher Risikotransfer nur gegen eine entsprechende Prämie möglich. Vorteil hierbei ist jedoch, dass der finanzielle Bedarf langfristig wirtschaftlich kalkulierbar ist. In vielen Situationen macht es daher Sinn, eine solche Prämie zu entrichten und im Gegenzug die Bedrohung eines existenzbedrohenden Risikos nicht mehr selbst tragen zu müssen. Eine Abwägung muss immer im Einzelfall vom Unternehmen selbst durchgeführt werden.

29.6 Fazit

Im Rahmen dieses Kapitels wurde zunächst die Wichtigkeit und Aktualität der Ermittlung des Terrorrisikos sowie der weiteren politischen Risiken erörtert. Im weiteren Verlauf wurde sowohl auf die Schwierigkeit der Risikoidentifizierung und -Messung wie auch auf die Probleme des Risikomanagementprozesses eingegangen. Hierzu wurde verschiedene qualitative und quantitative Methoden inklusive der jeweiligen Vor- und Nachteile dargestellt.

Die Ursachen für die entsprechenden Risiken sind nur schwer zu erkennen. Weiterhin liegen ihnen keine klaren Wahrscheinlichkeiten zu Grunde, was eine Risikokalkulation schwierig bzw. kaum möglich macht.

Im letzten Teil des Kapitels wurden verschiedene Risikomanagement-Methoden dargestellt. Hierbei wurde deutlich, dass Unternehmen viele aktive Möglichkeiten bei der Auswahl eines Standortes haben, um politischen Risiken, aber auch Terrorrisiken zu vermeiden oder zu minimieren. Weiterhin wurden Diversifikationsmethoden und Methoden zum Risikotransfer durch Versicherungen, erörtert.

Die zentrale Fragestellung, inwiefern Terrorrisiken und politische Risiken Auswirkungen auf multinationale Unternehmen haben können und wie diese identifiziert, gemessen und darüber hinaus in dem Risikomanagementprozess der Unternehmen einfließen können, wurde beantwortet. Weiterhin zeigen verschiedenste Beispiele aus der Vergangenheit und Gegenwart die Relevanz und Aktualität des Themas und somit auch die Wichtigkeit der Betrachtung der Risiken für das Risikomanagement insbesondere nationaler Unternehmen. Die angesprochenen Risiken und der Umgang mit ihnen werden daher auch in der Zukunft einen wesentlichen Einfluss auf den Erfolg oder Misserfolg unternehmerischer Tätigkeit haben.

Literatur

- Alderson, A. S. (2003). Globalisierung und die große Kehrtwende: Entwicklung der Einkommensungleichheiten in 16 OECD-Staaten. In W. Müller & S. Scherer (Hrsg.), *Mehr Risiken – mehr Ungleichheit? Abbau des Wohlfahrtsstaats* (S. 323 f.). Frankfurt/New York: Flexibilisierung der Arbeit und die Folgen.
- Aon. (2019). Aon risk maps – Aon's guide to political risk, terrorism & political violence. Aon in partnership with The Risk Advisory Group and Continuum Economics. <https://www.riskadvisory.com/campaigns/terrorism-political-violence-risk-map-2018/>. Zugegriffen am 22.06.2019.
- Ballais, S. (1985). *Die Bedeutung politischer Risiken für ausländische Direktinvestitionen*. Nürnberg: Pauli-Balleis.
- BERI. (2018). Business environment risk intelligence 2018. <http://www.beri.com/Publications/BRS.aspx>. Zugegriffen am 12.06.2019.
- Brink, C. H. (2016). *Measuring political risk: Risks to foreign investment*. Cape Town/Stellenbosch: Taylor and Francis Group/University of Stellenbosch.

- CIA. (2010). Title 22 – Foreign relations and intercourse § 2656 f (d). <https://www.govinfo.gov/content/pkg/USCODE-2010-title22/pdf/USCODE-2010-title22-chap38-sec2656f.pdf>. Zugriffen am 16.06.2019.
- Diekmann, M. (2002). Direktinvestitionen im internationalen Wirtschaftsrecht, aus den Wissensarchiven von GRIN. München: Grin.
- FBI. (2019). Terrorism 2002–2005. U.S. Department of Justice, Federal Bureau of Investigation. <https://www.fbi.gov/stats-services/publications/terrorism-2002-2005>. Zugriffen am 16.06.2019.
- GTD. (2018). Global Terrorism Database, University of Maryland. <https://www.start.umd.edu/gtd/>. Zugriffen am 12.06.2019.
- de Haan, H. (1984). *Die Risikopolitik der internationalen Unternehmung, Pausenberg, von Ehrenfried*. Wolfgang: Verlag der Ferberschen Universitätsbuchhandlung Gießen.
- Howell, L. D. (2001). *The handbook of country and political risk analysis* (3. Aufl.). East Syracuse: The PRS Group.
- Köpplinger, H. (1986). *Risiken im Auslandsgeschäft* (B. Siegfried, Hrsg.). Nürnberg: Pauli-Balleis.
- MIGA. (2017). Miga annual report 2017, MIGA.
- Naini. (1979). *Die Revolution im Iran* (S. 15 ff.). Hamburg: Dt. Orient Institut.
- Pabst, C. (2008). *Die Versicherbarkeit des Terrorismusrisikos: Eine qualitative Analyse der Versicherbarkeitskriterien und die versicherungswirtschaftliche Risikobewältigung mit mehreren Risikoträgern*. Saarbrücken: VDM Verlag Dr. Müller.
- PRS-Group. (2018). *International country risk guide methodology*. PRS Group.
- RMS. (2014). Terrorism modeling 101. RMS. <https://www.rms.com/blog/2014/12/17/terrorism-modeling-101/>. Zugriffen am 18.06.2019.
- Schneider, F., et al. (2008). *Ursachen und Wirkung des weltweiten Terrorismus – Eine Analyse der gesellschaftlichen und ökonomischen Auswirkungen und neuen Ansätze zum Umgang mit dem Terror* (1. Aufl.). Wiesbaden: Der Deutsche Universitäts-verlag und der VS Verlag für Sozialwissenschaften.
- Spiegel. (2019). Anschlagsserie in Sri Lanka – Zahl der Todesopfer nach unten korrigiert. *spiegel.de*. <https://www.spiegel.de/politik/ausland/sri-lanka-zahl-der-todesopfer-der-anschlaege-an-ostern-nach-unten-korrigiert-a-1264473.html>. Zugriffen am 25.04.2019.
- Surminski, S. (2003). Terrorasmus und die Versicherungsbranche – Globale Trends und Reaktionen. *ZfV*, 8/15, 219 ff.
- Thomann, C. (2007). *Terrorversicherung, Risikomanagement und Regulierung* (Bd. 33, S. 169 f.). Karlsruhe: Versicherungswirtschaft GmbH.
- Versicherungspraxis. (2016). Politische Risiken im In- und Ausland. *Die Versicherungspraxis*, 2016(11).
- Vincent, E. (2017). Attentat du 13-Novembre: deux ans après, les révélations de l'enquête in Le Monde (11. Novembre 2017).
- Zajak, S., et al. (2018). Zwischen Reform und Revolution: Ergebnisse der Befragung von G20 Demonstrierenden am 02. Und 08. Juli 2017 in Hamburg. *Forschungsjournal Soziale Bewegung*, Klein, Legrand, Thomas, Rohwender, 30(4), Online Erschienen am 02.02.2018.

Leo Zagel studierte Jura an der Universität München. Seit 1974 war er in der Versicherungswirtschaft bei verschiedenen Versicherern (Allianz, Gerling und EXTREMUS) unter anderem als Vorstand oder Vorstandsvorsitzender tätig. Derzeit ist er Generalbevollmächtigter bei der EXTREMUS Versicherungs-AG.

Volker Steinmetz wechselte nach einem Lehramtsstudium an der TU Darmstadt in die Versicherungswirtschaft. Als Versicherungskaufmann arbeitete er im Bereich der industriellen Sachversicherung. In der Folge war er in verschiedenen Positionen für internationale Versicherungsunternehmen tätig. Seit 2006 leitet er den Vertrieb und das Underwriting der EXTREMUS Versicherungs-AG, den deutschen Terrorversicherer in Köln.

Hans Lange absolvierte seine Ausbildung zum Kaufmann für Versicherung und Finanzen in der LVM-Versicherungsagentur Rüenauver. Darauffolgend studierte er Versicherungswesen mit den Schwerpunkten Risikomanagement, Bilanzierung von Versicherungsunternehmen und Sachversicherung am Institut für Versicherungswesen der Technischen Hochschule Köln. Im Anschluss absolvierte er dort auch das Masterstudium Risk & Insurance. Während seiner Studienzeit arbeitete er als Werkstudent bei Carl Jaspers Versicherungskontor GmbH.



Travel Risk Management

30

Martin Gary und Tim Thomas

Zusammenfassung

Im folgenden Kapitel wird das Travel Risk Management internationaler Unternehmen näher erläutert. Es wird aufgezeigt, inwiefern der Arbeitgeber gesetzlich dazu verpflichtet ist, seinen Arbeitnehmer vor einer Entsendung ins Ausland vorzubereiten. Zudem werden neben den gesetzlichen Vorgaben weitere Vorteile eines funktionierenden Travel Risk Managements aufgezeigt. Des Weiteren werden die Gefahren für Mitarbeiter im Ausland näher definiert. Im Fokus stehen die Gesundheits- und Unfallrisiken sowie die Gefahr durch Kriminalität. In diesem Zusammenhang werden geeignete Präventionsmaßnahmen für die jeweiligen Risiken erörtert und ergänzend Hinweise zur Versicherung dieser Risiken aufgezeigt.

30.1 Motivation für ein Travel Risk Management

In Zeiten der Globalisierung ist es bei internationalen Unternehmen selbstverständlich, dass auch das Arbeitsumfeld internationalen Ansprüchen genügen muss. Die Entsendung von Mitarbeitern ins Ausland ist somit nichts Außergewöhnliches mehr. Insbesondere Deutschland, als mehrfacher Exportweltmeister, ist von dieser Thematik betroffen. Global Mobility wird zukünftig für international agierende Unternehmen ein immer relevante-

M. Gary
Albatros Versicherungsdienste GmbH, Köln, Deutschland
E-Mail: martin.gary@albatros.de

T. Thomas (✉)
TH Köln, Institut für Versicherungswesen, Köln, Deutschland
E-Mail: timthomas1@gmx.de

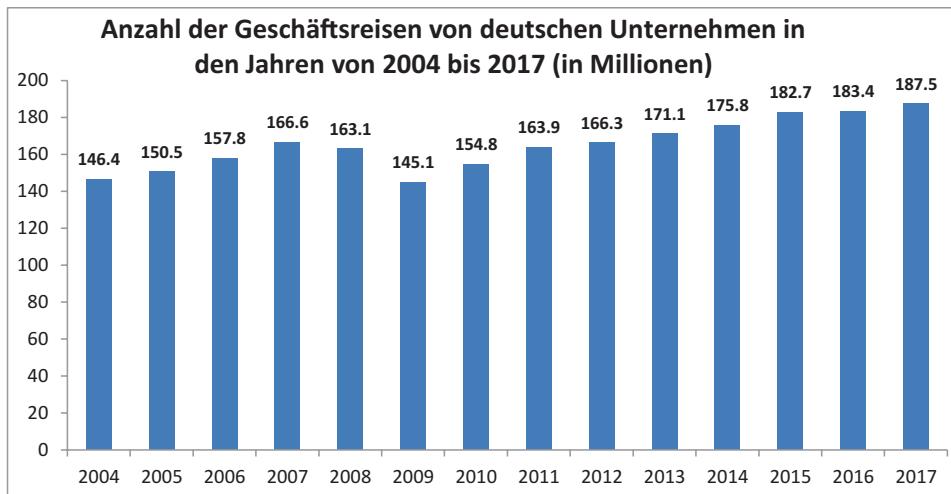


Abb. 30.1 Entwicklung der Anzahl deutscher Geschäftsreisen 2004 bis 2017. (Quelle: eigene Darstellung in Anlehnung an Verband Deutsches Reisemanagement [2018](#))

res Thema und demnach wird Mobilität und Flexibilität vermehrt auch von vielen Arbeitgebern als Einstellungskriterium vorausgesetzt. Im Jahr 2017 unternahmen Mitarbeiter deutscher Unternehmen ca. 187,5 Millionen Geschäftsreisen. Abb. 30.1 zeigt, dass die Anzahl der Geschäftsreisen zwischen 2007 und 2017 um mehr als 20 Millionen angestiegen ist (vgl. Verband Deutsches Reisemanagement [2018](#)).

Des Weiteren sehen viele Unternehmen für sich ein großes wirtschaftliches Potenzial in Schwellen- und Entwicklungsländern. Die Strukturen und Gegebenheiten vor Ort unterscheiden sich allerdings stark von denen in Deutschland. Daher ist ein funktionierendes Travel Risk Management unumgänglich (vgl. Trauboth et al. [2016](#), S. 268 f.). Der folgende Aufsatz befasst sich mit den Gefahren, denen Mitarbeiter während beruflicher Auslandsreisen oder Entsendungen unter Umständen ausgesetzt sein können und mit dem entsprechenden Riskmanagement-Prozess. Im Fokus stehen hierbei medizinische Risiken, eine erhöhte Unfallgefahr und der Umgang mit einer Bedrohung durch Kriminalität.

30.1.1 Rechtliche Verpflichtung des Arbeitgebers

Arbeitnehmer können ihren Arbeitgeber unter gewissen Umständen für die Folgen eines Krankheitsfalles oder eines Unfalls während einer Entsendung ins Ausland haftbar machen. Aus § 618 BGB in Verbindung mit § 241 Abs. 2 BGB ergeben sich Fürsorgepflichten des Arbeitgebers (vgl. Balme und Ruscheinsky [2017](#), S. 14). Der konkrete Umfang der Fürsorgepflichten des Arbeitgebers ist im Gesetz nicht definiert und richtet sich nach den jeweiligen Umständen und dem Zielland. Je mangelhafter die Versorgung im Zielland ist, desto höhere Anforderungen werden an die Fürsorgepflichten des Arbeitgebers gestellt (vgl. International SOS Foundation [2014](#), S. 22).

Sollte der Arbeitgeber seinen Mitarbeiter in Regionen entsenden, in denen bestimmte Gefahren herrschen, so hat er die Pflicht, ihn über die vorherrschenden Gefahren zu informieren. Informationen zur medizinischen Versorgung und zur Verkehrslage sind in dem Zusammenhang ebenso relevant wie Informationen zur politischen Lage oder zur Kriminalität in dem jeweiligen Land. Letzteres gilt besonders für krisengefährdete Gebiete, in denen der Mitarbeiter zum Beispiel einem (erhöhten) Entführungsrisiko ausgesetzt ist (vgl. Fuhlrott und Schröder 2017, S. 625 ff.).

Eine weitere wichtige Gesetzesnorm bezüglich der Haftung des Arbeitgebers liefert das fünfte Sozialgesetzbuch (SGB). Aus § 17 des SGB V geht hervor, dass der Arbeitgeber für medizinische Behandlungsmaßnahmen während der Entsendung finanziell aufkommen muss. Zudem sieht diese Regelung vor, dass der Arbeitgeber zusätzlich auch die Krankheitskosten von mitreisenden Familienangehörigen zu übernehmen hat (§ 17 SGB V Abs. 1 S. 2 in Verbindung mit § 10 SGB V). Die Krankenkasse erstattet lediglich die Höhe der Behandlungskosten, die unter den gleichen Umständen in Deutschland angefallen wären. Behandlungskosten im Ausland können jedoch stark von denen in Deutschland abweichen. In Ländern wie zum Beispiel den USA sind die Kosten für eine medizinische Behandlung um einiges höher als in Deutschland. Das stellt für das Unternehmen ein großes Problem dar, da solche Kosten im Vorhinein schlecht kalkuliert werden können. Daher empfiehlt sich der Abschluss einer internationalen Krankenversicherung (vgl. Baum 2017, S. 17). Kriterien, die beim Abschluss einer internationalen Krankenversicherung zu beachten sind, werden in Abschn. 30.2.3 näher erläutert.

Außerdem sollte vor der Entsendung die gesundheitliche und mentale Tauglichkeit des Mitarbeiters für den jeweiligen Auslandseinsatz festgestellt werden. Erfolgt dies nicht, können ggf. kostspielige Rückholmaßnahmen erforderlich sein (vgl. Pfannstiehl et al. 2019, S. 172). Mitreisende Familienangehörige sollten ebenfalls in die Vorbereitungen eingebunden werden. Je nach Art der Gefährdung kann es auch notwendig sein, besondere Sicherheitstrainings zu absolvieren. Insbesondere bei der Entsendung in Krisenländer, in denen Mitarbeiter einem potenziellen Entführungsrisiko ausgesetzt werden, sind solche Sicherheitstrainings unabdingbar (vgl. Trauboth et al. 2016, S. 88 f.). Weitere Informationen über die Pflichtvorsorge des Arbeitgebers werden in der „Verordnung zur arbeitsmedizinischen Vorsorge (ArbMedVV)“ spezifiziert. Bei Entsendungen in Tropengebiete muss zum Beispiel gemäß der ArbMedVV die Beratung durch einen ausgewiesenen Tropenmediziner oder einen Facharzt für Arbeitsmedizin erfolgen (vgl. ArbMedVV Anhang Teil 4). Hierauf wird in Abschn. 30.2.2 detaillierter eingegangen. Zusätzliche Anforderung an den Arbeitgeber stellt die „Deutsche Gesetzliche Unfallversicherung“ (DGUV). Die DGUV Vorschriften werden in Abschn. 30.3.2 näher beschrieben.

Sollten die Fürsorgepflichten nach § 241 Abs. 2 BGB nicht erfüllt werden, kann sich daraus ein berechtigter Schadensersatzanspruch gemäß § 280 Abs. 1 S. 2 BGB ergeben (vgl. Fuhlrott und Schröder 2017, S. 625 ff.). Bei dem Travel Risk Management und der Entsendung von Mitarbeitern ist jedoch nicht nur die juristische Betrachtung relevant. Im Folgenden wird erläutert, welche weiteren Aspekte von Bedeutung sind.

30.1.2 Weitere Motivation für ein effizientes Travel Risk Management

Neben der rechtlichen Verpflichtung und der damit einhergehenden Haftung des Arbeitgebers sind vor allem auch wirtschaftliche Aspekte ein schwerwiegendes Argument für die Investition in ein Travel Risk Management. Sollte ein entsandter Mitarbeiter krankheitsbedingt für einen längeren Zeitraum ausfallen, zum Beispiel weil er eine notwendige Impfung nicht erhalten hat, muss das Unternehmen unter Umständen mit hohen Umsatzeinbußen rechnen. Entsandte Mitarbeiter sind häufig fachlich hoch qualifiziert und somit schwer zu ersetzen (vgl. Pfannstiehl et al. 2019, S. 170). Hinzu kommen Investitionen in die Entsendung des Mitarbeiters (zum Beispiel Vorbereitungsmaßnahmen, Flüge etc.), die nicht den gewünschten Erfolg erzielt haben.

Des Weiteren dürfen die immateriellen Schäden einer gescheiterten Entsendung nicht außer Acht gelassen werden. Aufgrund versäumter Vorbereitungsmaßnahmen und dem daraus resultierenden Ausfall eines Mitarbeiters kann die eigene Firma in der Außenwirkung als unzuverlässig oder nicht ausreichend kompetent erscheinen. So können zum Beispiel Geschäftsbeziehungen oder die Unternehmensreputation geschädigt werden (vgl. Hechler 2015, S. 38). Eine Studie der DGUV hat den wirtschaftlichen Nutzen von Präventionsmaßnahmen analysiert und quantifiziert. Die DGUV ist zu dem Ergebnis gekommen, dass jedem Euro, der in Präventionsmaßnahmen investiert wird, ein Präventionsnutzen von 2,20 Euro gegenübersteht (Deutsche Gesetzlichen Unfallversicherung – DGUV 2013, S. 34).

Viele Unternehmen entscheiden sich dafür, ihre Mitarbeiter über die gesetzlichen Anforderungen hinaus zu unterstützen. Der Begriff „Corporate Social Responsibility“ beschreibt unter anderem die unternehmerische Verantwortung in Bezug auf soziale Werte und den nachhaltigen Umgang mit Ressourcen. Dies betrifft auch die Verantwortung gegenüber den eigenen Mitarbeitern, insbesondere in solchen Extremsituationen wie einer Entsendung ins Ausland (vgl. Karlshaus et al. 2019, S. 2 ff.).

In Zeiten, in denen „Corporate Social Responsibility“ fest in die Managementprozesse großer Unternehmen eingebunden ist, wird darauf Wert gelegt, dass sich der Mitarbeiter jederzeit unterstützt und wertgeschätzt fühlt. Der Arbeitgeber signalisiert dem Mitarbeiter durch umfangreiche Vorbereitungsmaßnahmen für die Entsendung, dass er sich um das Wohl des Mitarbeiters sorgt. Dies kann zum Beispiel durch angebotene Sprachkurse, Sicherheitstrainings oder einen umfangreichen Versicherungsschutz erfolgen. Besondere interkulturelle Trainings dienen dazu, die Mitarbeiter auf die bevorstehenden Herausforderungen vorzubereiten und die Reise in das bisher unbekannte Land gut vorbereitet und mit einem guten Gefühl anzutreten. Sollte der Mitarbeiter zum Beispiel nicht ausreichend auf kulturelle Unterschiede hingewiesen werden, so kann ein Kulturschock folgen, der im schlimmsten Fall sogar zu einem Burn-out führen kann (vgl. Karlshaus et al. 2019, S. 38).

Durch eine umfangreiche Vorbereitung des Mitarbeiters auf seine Entsendung (ggf. auch über die gesetzliche vorgeschriebene Fürsorgepflicht hinaus) erfolgt somit, dank der dadurch gesteigerten Motivation des Mitarbeiters, eine bessere Arbeitsleistung. Viele Studien belegen, dass Unternehmen, die großen Wert auf „Corporate Social Responsibility“

und „Employer Branding“ legen, aus betriebswirtschaftlicher Sicht erfolgreicher sind (vgl. Bungard 2018, S. 149 f.). Zudem erhält das Unternehmen eine bessere Reputation. Sollte das Unternehmen die Fürsorgepflichten nicht ausreichend erfüllen und als Folge dessen der Mitarbeiter verletzt werden, so kann dies negative Presse hervorrufen und abschreckend auf zukünftige, potenzielle Arbeitnehmer wirken (International SOS Foundation 2014, S. 4). Nachdem in diesem Abschnitt die Motivationen für ein Travel Risk Management erläutert wurden, werden im Folgenden die konkreten Gefahren und Maßnahmen dargelegt. Zudem werden ergänzend Versicherungslösungen aus der privaten Versicherungswirtschaft analysiert. Die Komponente der Sozialversicherung ist nicht Bestandteil dieses Kapitels, da diese einen separaten Themenkomplex darstellt, der eigens analysiert werden muss.

30.2 Schutz des Mitarbeiters vor Krankheiten während einer Entsendung ins Ausland

30.2.1 Medizinische Risiken

Die medizinischen Risiken hängen vom jeweiligen Land der Entsendung ab. In asiatischen, afrikanischen oder südamerikanischen Ländern sind entsandte Mitarbeiter im Vergleich zu europäischen Ländern höheren Gesundheitsrisiken ausgesetzt (vgl. Pfannstiehl et al. 2019, S. 178). Neue klimatische Gegebenheiten (zum Beispiel Luftfeuchtigkeit und Hitze) können für Menschen aus anderen Regionen belastend sein. Ein gesunder Mensch gewöhnt sich jedoch in der Regel an das neue Klima und ist diesen Belastungen gewachsen. Andere Veränderungen im Umfeld können jedoch weitaus gefährlicher sein. Besondere Einwirkungen auf den entsandten Mitarbeiter haben die örtlichen Hygienestandards, die Infrastruktur der lokalen medizinischen Versorgung oder die Verbreitung von Infektionskrankheiten. Des Weiteren sind kulturelle Unterschiede zum Herkunftsland ein relevanter Faktor, da gravierende kulturelle Unterschiede zu psychischen Erkrankungen des entsandten Mitarbeiters führen können (vgl. Pfannstiehl et al. 2019, S. 183 ff.).

Mangelnde Hygiene kann weitreichende Folgen haben. Insbesondere in warmen Ländern liegen die Hygienestandards häufig unter dem deutschen Niveau. Das warme Klima begünstigt die Vermehrung von Bakterien, Würmern oder Parasiten. Somit kommen potentielle Krankheitserreger und Infektionsherde häufiger vor. Restaurants müssen Speisen unter schlechteren hygienischen Bedingungen zubereiten, als es in Deutschland der Fall ist. Das kann nach dem Verzehr zum Beispiel zu Magen-Darm-Erkrankungen führen. Zudem ist in einigen Ländern das Wasser aus städtischen Leitungen häufig verunreinigt und kann nicht als Trinkwasser genutzt werden. Es besteht die Gefahr von Keimen oder Legionellen (vgl. Pfannstiehl et al. 2019, S. 183 ff.).

Besonders in Entwicklungs- oder Schwellenländern kann die medizinische Versorgung durch Ärzte oder in Krankenhäusern weit unter dem deutschen Standard liegen (vgl. Ipsos Institute 2018, S. 11). Dies kann sich unter anderem in einer mangelhaften Ausbildung des

ärztlichen Personals, unzureichender Hygiene in Krankenhäusern oder defizitärer Versorgung von Medikamenten widerspiegeln. Infektionskrankheiten durch die Nutzung nicht steriler Nadeln sind ein weit verbreitetes Phänomen. Zudem besteht die Gefahr einer Übertragung von Viren oder Bakterien durch die Bluttransfusion von Fremdblut. Besonders gefährlich in dem Zusammenhang ist die Ansteckung mit Hepatitis oder dem „Humanen Immundefizienz-Virus“ (HIV).

Eine der weitverbreitetsten Infektionskrankheiten in Tropengebieten ist Malaria. Im Jahr 2017 infizierten sich ca. 219 Millionen Menschen mit der Krankheit. Somit ist Malaria die am häufigsten auftretende Infektionskrankheit weltweit. Kinder reagieren besonders anfällig auf die Krankheit. Aus dem „World Malaria Report 2018“ der World Health Organization geht hervor, dass alle zwei Minuten ein Kind an den Folgen einer Malaria-Infektion stirbt. Die Krankheit wird durch den Stich weiblicher Stechmücken übertragen (vgl. World Health Organization 2018, S. 4).

Eine Entsendung kann für den Mitarbeiter neben Einwirkungen auf die physische Gesundheit auch Einwirkungen auf die Psyche haben. Je nach Zielland kann es unter Umständen sein, dass der entsandte Mitarbeiter mit für ihn unbekannten Kulturen und Mentalitäten konfrontiert wird. Es besteht die Gefahr eines Kulturschocks. Ein Kulturschock „beschreibt die psychischen Folgen einer mangelnden Anpassung an das Ausland insbesondere in den ersten Monaten des Aufenthalts“ (vgl. Karlshaus et al. 2019, S. 37).

Nach anfänglicher Euphorie (man spricht von der sogenannten Honeymoon-Phase) sinkt die Zufriedenheit des entsandten Mitarbeiters schnell. Fehlende soziale Kontakte oder gravierende kulturelle Unterschiede wirken sich negativ auf die Psyche aus. In Extremfällen kann dies sogar zu psychischen Krankheiten wie Burn-Out oder Depressionen führen. Das gewohnte soziale Umfeld, mit dem im Herkunftsland Sorgen und Probleme geteilt und gelöst werden, ist während einer Entsendung weit entfernt. Zudem lässt sich professionelle psychologische oder psychiatrische Hilfe in manchen Ländern nur schwer finden bzw. ist aufgrund von Sprachbarrieren nicht durchführbar. In extremen Fällen kann es zu einem Abbruch der Entsendung kommen (vgl. Pfannstiel et al. 2019, S. 191). In der Regel gewöhnt sich der Mitarbeiter jedoch an die Umstände und findet sich mit den örtlichen Gegebenheiten ab. Sollte es sich um eine längere Entsendung handeln, kann auch die Rückkehr ins Heimatland mit einer schwierigen Eingewöhnungsphase verbunden sein. In solchen Fällen spricht man von einem doppelten Kulturschock (vgl. Karlshaus et al. 2019, S. 39).

Abb. 30.2 stellt die verschiedenen Phasen der Entsendung grafisch dar und zeigt auf, dass geeignete Vorbereitungsmaßnahmen den Einfluss eines Kulturschocks auf das Wohlbefinden des Mitarbeiters mindern.

30.2.2 Präventionsmaßnahmen

Allgemein ist festzustellen, dass eine gute und zielgerichtete Vorbereitung des Mitarbeiters die Basis für eine erfolgreiche Entsendung ist. Davor ist jedoch die Auswahl eines

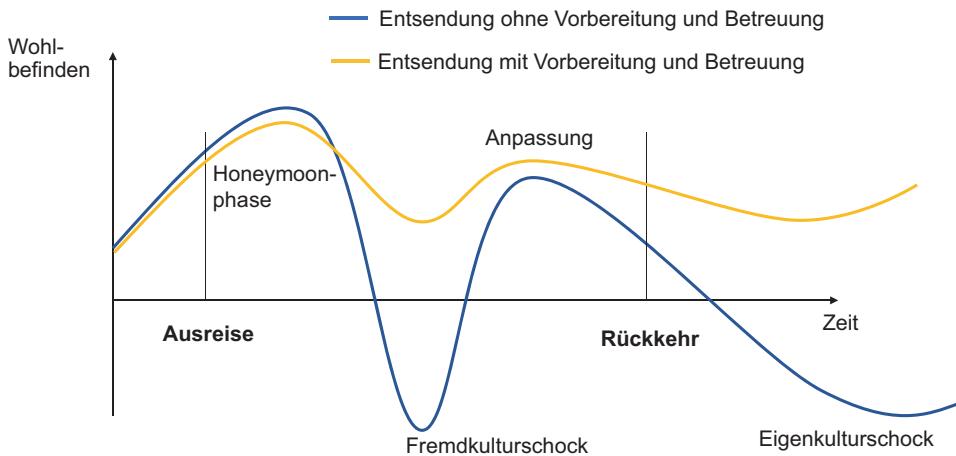


Abb. 30.2 Wohlbefinden des entsandten Mitarbeiters im Zeitverlauf der Entsendung. (Quelle: eigene Darstellung in Anlehnung an Karlshaus et al. 2019, S. 39)

passenden Mitarbeiters erforderlich. Eine sorgfältige Prüfung der körperlichen Gesundheit ist unerlässlich. Sollten chronische Krankheiten bekannt oder der Mitarbeiter auf die regelmäßige Einnahme von Medikamenten angewiesen sein, so muss geprüft werden, ob die medizinische Versorgung in der jeweiligen Region gewährleistet ist. Neben der körperlichen Verfassung werden von entsandten Mitarbeitern auch gewisse Kompetenzen gefordert. Auf diese sollte bei der Auswahl der jeweiligen Mitarbeiter besonders geachtet werden. Eine ausgeprägte Flexibilität, Kommunikationsfähigkeit und Offenheit sind entscheidend für eine stabile psychische Verfassung während der Entsendung. Ebenso wichtig sind ein interkulturelles Wissen und eine gewisse Selbstsicherheit. Mitarbeiter, die durch diese Kompetenzen herausstechen, sind weniger anfällig für psychische Krankheiten wie Depressionen oder Burn-Out während der Entsendung (vgl. Karlshaus et al. 2019, S. 39).

Bei einer Mitarbeiterentsendung in tropische Gebiete, Gebiete mit besonderen klimatischen Belastungen oder Gebiete mit hohen Infektionsgefährdungen, gelten gemäß der ArbMedVV besondere Bestimmungen. Der Arbeitgeber hat dafür Sorge zu tragen, dass der Mitarbeiter sich vor der Entsendung von einem ausgewiesenen Tropenarzt oder einem Facharzt für Arbeitsmedizin aufklären und ggf. behandeln lässt. Sollte die Familie des Mitarbeiters diesen bei der Entsendung begleiten, so gilt dies auch für die jeweiligen Familienmitglieder (vgl. ArbMedVV Anhang Teil 4). Im Vordergrund einer solchen Beratung steht eine erforderliche Impfprophylaxe. Vorbeugende Maßnahmen, um eine Malaria-Infektion zu vermeiden, sind in der Regel auch elementarer Bestandteil der Beratung durch einen Tropenarzt. So sollten dem Mitarbeiter Informationen zu Symptomen, Übertragung und Verhaltenspräventionen übermittelt werden. Zudem erfolgt meist eine medikamentöse Prophylaxe (vgl. Deutsche Verbindungsstelle Unfallversicherung – Ausland (DVUA) 2018, S. 37).

Um den Mitarbeiter mental auf die Entsendung vorzubereiten, eignen sich besonders sogenannte „look-and-see“ Reisen. Der Mitarbeiter, der entsandt werden soll, besucht für ein bis zwei Wochen das Zielland und bekommt einen ersten Eindruck davon, ob er sich vorstellen kann dort zu leben und zu arbeiten. Sollte die Familie ihn bei der Entsendung begleiten, sind sie auch in diese Maßnahme einzubeziehen. Studien belegen, dass die Unzufriedenheit des Partners einer der häufigsten Gründe für den Abbruch einer Entsendung ist (vgl. Baum 2017, S. 20). Häufig steht die Entsendung vor einer solchen Reise schon fest und die entsprechenden Verträge sind schon unterzeichnet. In dem Fall dient die Reise dazu, Wohnverhältnisse zu klären, ggf. einen Schul- oder Kindergartenplatz zu finden oder weitere potenzielle Problemfelder zu identifizieren (vgl. Bereuter-Hämmerle 2016, S. 31).

Wie eingangs erwähnt hat der Arbeitgeber im Rahmen seiner Fürsorgepflichten die Aufgabe, den Arbeitnehmer vor einer Entsendung über potenzielle Gefahren oder kulturelle Besonderheiten aufzuklären. Dies kann intern erfolgen, zum Beispiel durch Mitarbeiter, die selber schon einen längeren Zeitraum im jeweiligen Land gearbeitet haben. Eine weitere Möglichkeit ist ein interkulturelles Training durch einen externen Dienstleister. Diese weisen häufig eine Spezialisierung für bestimmte Gebiete oder Länder auf und besitzen detailliertes Wissen zu den lokalen Gegebenheiten der jeweiligen Region. Ziel eines solchen interkulturellen Trainings ist nicht nur das Wissen über die kulturellen Unterschiede, sondern vielmehr der Umgang mit diesen (vgl. Bereuter-Hämmerle 2016, S. 26).

Trotz der besten Präventionsmaßnahmen kann es jedoch immer zu einem Krankheitsfall kommen, der eine medizinische Behandlung erfordert. Um eine adäquate medizinische Behandlung des entsandten Mitarbeiters zu gewährleisten, ist eine internationale Krankenversicherung von Vorteil. Diese bietet neben der bloßen Krankenkostenerstattung auch Serviceleistungen durch ein internationales Netzwerk. Im folgenden Abschnitt werden die Bestandteile einer solchen erläutert.

30.2.3 Versicherungslösungen

Wie bereits in Abschn. 30.1.1 erörtert, gelten für den Arbeitgeber die gesetzlichen Fürsorgepflichten, an die er sich zwingend halten muss (vgl. § 618 BGB in Verbindung mit § 241 Abs. 2 BGB). Diese gelten auch für die medizinische Versorgung des Mitarbeiters. Konkreter noch: Der Arbeitgeber hat sich im Rahmen der gesetzlichen Fürsorgepflichten nicht nur um Prävention zu bemühen, sondern muss finanziell auch für eine medizinische Behandlung des entsandten Mitarbeiters und seiner mitreisenden Familienangehörigen aufkommen (vgl. Baum 2017, S. 17 und § 17 SGB V). Daher ist der Abschluss einer internationalen Krankenversicherung durch das Unternehmen sehr zu empfehlen.

Diese übernimmt die Kosten für die medizinische Behandlung und notwendige Arzneimittel. Abhängig von der Anzahl der entsandten Mitarbeiter bieten sich Gruppenverträge an. In diesem Fall ist das jeweilige Unternehmen der Versicherungsnehmer und die versicherten Personen sind die entsandten Mitarbeiter und deren Familienangehörigen. Sollten vor der Entsendung „look-and-see“ Reisen geplant sein, so gilt es sicherzustellen, dass zu

diesem Zeitpunkt bereits der Versicherungsschutz greift. Viele Krankenversicherer bieten Online-Tools an, in denen es den Unternehmen auf einfache Weise möglich ist, die jeweiligen Mitarbeiter an- bzw. abzumelden. Dies erspart dem Unternehmen administrativen Aufwand (vgl. Baum 2017, S. 19). Auch der Mitarbeiter hat Zugriff auf die Online-Tools und ist so in der Lage, jederzeit persönliche Inhalte (z. B. Datenschutzgrundverordnungsvereinbarung oder Tarife) einzusehen. Für kurzzeitige Dienstreisen existieren am Markt auch Policen, in denen jeder reisende Mitarbeiter ohne An- oder Abmeldung pauschal mitversichert ist.

Anbieter von internationalen Krankenversicherungen können sich im Hinblick auf ihre Bedingungen und Leistungen stark voneinander unterscheiden. Daher gilt es vor Abschluss zu prüfen, ob alle relevanten Leistungsbausteine mitversichert sind. Eine wichtige Klausel ist die freie Arzt- bzw. Krankenhauswahl. Häufig bieten öffentliche Krankenhäuser im Ausland nicht den aus Deutschland gewohnten Standard. Private Kliniken sind meist umfangreicher ausgestattet und bieten einen besseren Service. Daher sollte darauf geachtet werden, dass im Notfall auch die Behandlungskosten in solchen vollständig übernommen werden (vgl. Baum 2017, S. 19).

Zudem besteht bei einigen Tarifen für kurzzeitige Dienstreisen ein Ausschluss von Vorerkrankungen in den Bedingungen der Auslandsreisekrankenversicherung. Häufig hängen Vorerkrankungen und die medizinische Behandlung im Ausland kausal zusammen. Damit das Unternehmen in so einem Fall eine Erstattung der Behandlungskosten erhält, empfiehlt sich eine Auslandsreisekrankenversicherung ohne den Ausschluss von Vorerkrankungen.

Sollte es dem Mitarbeiter während der Entsendung aufgrund gesundheitlicher Umstände nicht mehr zumutbar sein, sich weiterhin im Ausland aufzuhalten, ist ein Rücktransport erforderlich. Dieser ist mit finanziellen Aufwendungen für den Arbeitgeber verbunden. Der Rücktransport ist Bestandteil von internationalen Krankenversicherungs-Policen. Insbesondere bei der Rücktransport-Klausel unterscheiden sich jedoch einige Versicherungen. So werden bei vielen Versicherern die Kosten für einen Rücktransport nur erstattet, falls dieser medizinisch „notwendig“ ist und durch einen Arzt angeordnet wird. Als medizinisch notwendig gilt ein Rücktransport, wenn der medizinische Standard in dem Land der Entsendung so niedrig ist, dass eine adäquate Behandlung nicht möglich ist. Dies ist in der Praxis nur äußerst selten der Fall. In anderen Klauseln findet sich hingegen die Formulierung, dass eine Erstattung der Kosten für den Rücktransport erfolgt, wenn dieser medizinisch „sinnvoll“ ist. Diese Formulierung ist wesentlich weiter und für das versicherungnehmende Unternehmen positiver gefasst. Die Rücktransporte werden von spezialisierten Dienstleistern durchgeführt, wie zum Beispiel Lufthansa oder ADAC. Durch Flugzeuge, die mit sogenannten „Medical Cabins“ ausgestattet sind, ist es möglich, während längerer Flüge eine umfassende medizinische Behandlung zu gewährleisten.

Sollten Mitarbeiter in Krisenregionen entsendet werden, ist die Formulierung der sogenannten Kriegsklausel von besonderer Bedeutung. Man unterscheidet zwischen dem aktiven und dem passiven Kriegsrisiko. Das aktive Kriegsrisiko beschreibt die aktive Teilnahme an beispielsweise gewalttätigen Demonstrationen oder Waffengebrauch. Daraus

resultierende Gesundheitsschäden sind grundsätzlich vom Versicherungsschutz ausgeschlossen. Es sollte jedoch darauf geachtet werden, dass Versicherungsschutz besteht, wenn sich der Mitarbeiter lediglich in einem solchen Land aufhält, ohne in irgendeiner Weise aktiv an einem Kriegsgeschehen teilzunehmen. Hierbei wird von dem passiven Kriegsrisiko gesprochen (vgl. Baum 2017, S. 20).

Neben der reinen Kostenübernahme fungieren viele Versicherer mittlerweile auch als Dienstleister. Der Versicherer steht dem Unternehmen bzw. dem Mitarbeiter im medizinischen Notfall als Partner zur Seite und unterstützt ihn dabei, eine optimale medizinische Versorgung zu gewährleisten. Hierbei helfen beispielsweise mehrsprachige 24-Stunden-Hotlines, über die der Mitarbeiter im Ernstfall Kontakt zu Spezialkliniken herstellen kann. Insbesondere bei Mitarbeitern, die des Öfteren Dienstreisen in unterschiedlichen Ländern unternehmen, ist es hilfreich, im Notfall einen Ansprechpartner zu haben, der über ein globales Netzwerk verfügt. Vorteile eines solchen globalen Netzwerkes sind neben dem Kontakt zu geprüften Ärzten und medizinischen Einrichtungen auch ein einfacher Abrechnungsvorgang. Häufig ist es möglich, dass der Versicherer direkt mit dem örtlichen Arzt oder Krankenhaus abrechnet und der Arbeitnehmer somit nicht in Vorleistung gehen muss (vgl. Baum 2017, S. 19).

Als Schnittstelle zwischen Versicherern, Versicherungsnehmern und Krankenhaus/Arzt gelten sogenannte „Third Party Administrators“ (TPA). Diese ermöglichen erst die globalen Netzwerke, da die meisten deutschen Versicherer allein über solche Kapazitäten nicht verfügen. Insbesondere durch die effiziente Zahlungsabwicklung, die die TPAs ermöglichen, erfolgt eine enorme Kosteneinsparung, die sich auch in den Versicherungsprämien widerspiegelt.

Neben der Gefahr durch Krankheiten existiert in vielen Ländern auch eine erhöhte Unfallgefahr. Im folgenden Abschnitt werden sowohl die Ursachen für eine erhöhte Unfallgefahr als auch die Unfallprävention im Ausland näher erläutert.

30.3 Unfallschutz bei der Entsendung ins Ausland

30.3.1 Unfallursachen während einer Entsendung

Das gravierendste Problem bei den innerbetrieblichen Risiken in vielen Ländern ist, dass sich die lokalen Sicherheitsstandards häufig von denen in Deutschland unterscheiden. Insbesondere in Entwicklungsländern oder Schwellenländern liegen diese weit unter dem deutschen Niveau. Es fehlt an fachlichem Know-how und Ressourcen bezogen auf den Arbeitsschutz (vgl. Bundesanstalt für Arbeitsschutz und Arbeitsmedizin 2016, S. 59).

Das Unfallrisiko kann bereits auf dem Weg zum Arbeitsplatz beginnen. Unfälle im Straßenverkehr zählen zu den fünf häufigsten Gründen für Evakuierungen aus dem Ausland (International SOS Foundation 2018). Unter Umständen sind die Verkehrswege oder auch die Verkehrsmittel unsicherer als in Deutschland. Der Mitarbeiter befindet sich auf ungewohnten Straßen in einem für ihn unbekannten Land. Allein diese Tatsache kann

schon zu einer erhöhten Unfallgefahr führen. Wenn zusätzlich die Fahrbahn oder die Beschilderung eine verminderte Qualität aufweisen, als es der Mitarbeiter aus Deutschland gewohnt ist, führt dies zu einer erhöhten Gefahr eines Wegeunfalls. Auch der öffentliche Personennahverkehr birgt Gefahren, da hier ebenfalls in vielen Ländern andere Sicherheitsstandards und Regularien herrschen (vgl. Pfannstiehl et al. 2019, S. 186).

Ähnliches gilt auch für die Unfallrisiken am unmittelbaren Arbeitsplatz. Abhängig von der ausgeübten Tätigkeit variiert dieses Risiko. Häufig werden Mitarbeiter nicht ausreichend in ihre Tätigkeit eingewiesen (vgl. Balme und Ruscheinsky 2017, S. 15). Hinzu kommt, dass Notfallhelfer ggf. nicht ausreichend geschult sind, um im Ernstfall adäquate Erste-Hilfe-Maßnahmen einzuleiten. Im schlimmsten Fall stehen gar keine Notfallhelfer zur Verfügung. Neben den Notfallhelfern mangelt es häufig auch an der passenden und ausreichenden Ausstattung, um Notfallhilfe leisten zu können. Zudem ist ein zeitnahe Notfalltransport nicht in allen Ländern gewährleistet (International SOS Foundation 2014, S. 27 f.; Pfannstiehl et al. 2019, S. 186).

Eine weitere relevante Gefahrenquelle für Unfälle sind die Werkzeuge und Maschinen vor Ort. Regelmäßige Wartungen sind kostenintensiv und ggf. nicht in dem Ausmaß vom Gesetz vorgeschrieben, wie es in Deutschland der Fall ist. Daher könnten Maschinen oder Werkzeuge nicht mehr in einwandfreiem Zustand sein und der Mitarbeiter könnte sich an diesen verletzen (vgl. International SOS Foundation 2019, S. 19). Im folgenden Abschnitt werden Präventionsmaßnahmen, welche Arbeits- oder Wegeunfälle verhindern können, vorgestellt.

30.3.2 Präventionsmaßnahmen

Die Prävention von Unfällen im Zielland muss auf zwei Ebenen stattfinden. Sowohl der Mitarbeiter, dem die Entsendung bevorsteht, als auch das Unternehmen im Ausland müssen geeignete präventive Maßnahmen treffen. Das Unternehmen muss dabei im ersten Schritt die Unfallrisiken im Entsendungsland identifizieren und analysieren. Hierbei kann dem Arbeitgeber auch der jeweilige Träger der gesetzlichen Unfallversicherung helfen (vgl. Balme und Ruscheinsky 2017, S. 14). In einigen Fällen ist es durch die DGUV-Vorschriften vorgeschrieben, dass Auslandsaufenthalte der Mitarbeiter bei der DGUV angemeldet werden. Dies tritt häufig in der Baubranche auf (zum Beispiel DGUV Vorschrift 38 und 39). Die Anmeldepflicht existiert, damit bereits vor der Tätigkeit im Ausland gewisse Sicherheitsstandards geprüft und gewährleistet werden können (vgl. Deutsche Verbindungsstelle Unfallversicherung – Ausland (DVUA) 2018, S. 33 f.).

Wie bereits im vorherigen Abschnitt erläutert, stellt das Risiko von Verkehrsunfällen eine elementare Gefahr dar. Dieses Risiko kann minimiert werden, indem zum Beispiel Shuttleservices zwischen dem Hotel oder der Wohnung des Mitarbeiters und der Arbeitsstelle eingerichtet werden. Hierfür sollten ortskundige und vertrauenswürdige Bus- oder Taxiunternehmen engagiert werden, deren Fahrer der deutschen oder zumindest der englischen Sprache mächtig sind (vgl. International SOS Foundation 2014, S. 31).

Bereits vor Aufnahme der Tätigkeit im Ausland sollte sich das Unternehmen darüber informieren, wo sich in der Nähe der Arbeitsstelle Spezialkliniken oder Fachärzte befinden, die bei einem möglichen Unfall eine medizinische Behandlung vornehmen können. Unter Umständen lassen sich sogar deutsche oder deutschsprachige Ärzte finden. Diese Informationen sollten sowohl dem jeweiligen Mitarbeiter als auch dem Führungspersonal im Ausland zugänglich gemacht werden. Im Idealfall werden die wichtigsten Telefonnummern und Anschriften an geeigneter Stelle ausgehängt (vgl. International SOS Foundation 2014, S. 27 f.).

Arbeitet der entsandte Mitarbeiter in der Produktion oder auf einer Baustelle, so ist sicherzustellen, dass eine entsprechende Schutzkleidung vor Ort gewährleistet ist. So gehören zum Beispiel Sicherheitsschuhe oder Helme in Deutschland zur Normalität auf Baustellen, im Ausland kann das jedoch anders sein. Zudem ist es möglich, dass der Mitarbeiter seine Arbeit mit neuen Werkzeugen oder Maschinen verrichten muss, die ihm vorher nicht bekannt waren. Der Mitarbeiter muss im Umgang mit diesen geschult und auf die Gefahren aufmerksam gemacht werden. Ähnliches gilt für den Umgang mit Gefahrstoffen oder Chemikalien. Zudem gilt es sicherzustellen, dass sich sämtliche Maschinen und Werkzeuge in einem intakten Zustand befinden und gemäß Prüffristen ordnungsgemäß gewartet wurden (vgl. International SOS Foundation 2019, S. 19 ff.).

Abschließend ist festzuhalten, dass das Hauptziel sein sollte, die Sicherheitsstandards am Arbeitsplatz im Ausland an deutsche Verhältnisse anzupassen. Da sich dies in der Praxis schwierig gestalten kann und unzweifelhaft in einigen Ländern ein höheres Unfallrisiko als in Deutschland herrscht, empfiehlt sich der Abschluss einer Unfallversicherung für den Arbeitnehmer. Im folgenden Abschnitt werden die Bestandteile und Leistungen einer solchen näher ausgeführt.

30.3.3 Versicherungslösungen

Bei der Versicherung von mehreren Mitarbeitern empfiehlt sich der Abschluss einer Gruppenunfallversicherung. Ähnlich wie bei Gruppenverträgen in der Krankenversicherung ist bei einem Gruppenvertrag in der Unfallversicherung der Versicherungsnehmer das jeweilige Unternehmen und die versicherte Person der jeweilige Mitarbeiter. Der Versicherungsschutz besteht für den Mitarbeiter so lange, bis er das Unternehmen verlässt.

Die meisten Verträge bieten mittlerweile weltweiten Versicherungsschutz rund um die Uhr an, sodass der Mitarbeiter nicht nur am Arbeitsplatz versichert ist, sondern auch bei Freizeitaktivitäten. Es gibt keine gravierenden Unterschiede in den Leistungen zwischen einer Gruppenunfallversicherung eines in Deutschland lebenden Arbeitnehmers oder eines entsandten Arbeitnehmers, da der Versicherungsschutz einer Gruppenunfallversicherung weltweit gegeben ist (vgl. Gesamtverband der Deutschen Versicherungswirtschaft (GDV) 2014, S. 4). Es können jedoch Unterschiede zu privaten Unfallversicherungen hinsichtlich der versicherten Leistungen bestehen. So ist es zum Beispiel üblich, dass bei der privaten Unfallversicherung ein Tagegeld mitversichert wird. Bei Gruppenunfallversiche-

rungen tritt dies jedoch seltener auf, da dieser Zusatzbaustein den Unternehmen meist zu preisintensiv ist.

Auch die Definition des Unfallbegriffs unterscheidet sich nicht. So ist dieser durch den GDV wie folgt definiert: „Ein Unfall liegt vor, wenn die versicherte Person durch ein plötzlich von außen auf ihren Körper wirkendes Ereignis (Unfallereignis) unfreiwillig eine Gesundheitsschädigung erleidet“ (GDV 2014, S. 4).

Die einzelnen Leistungsbausteine können beliebig ausgewählt werden. So ist zum Beispiel eine einmalige Zahlung im Falle einer Invalidität denkbar. Diese wird gestaffelt und je nach Invaliditätsgrad ausgezahlt. Ersatzweise könnte eine Unfallrente vereinbart werden, die ab einem bestimmten Invaliditätsgrad ausgezahlt wird. Die Höhe dieser Leistungen ist individuell zu vereinbaren. Weitere feste Bestandteile von Unfallversicherungspolicen sind Sterbegelder, Kostenerstattungen von kosmetischen Operationen nach Unfällen oder Bergungskosten (vgl. GDV 2014, S. 4 ff.). Mitarbeiter, die sich für eine Entsendung bereit erklären, erwarten, dass ihre Hinterbliebenen im Falle eines tödlichen Unfalls abgesichert sind. Arbeitgeber, die dies ihren Mitarbeitern nicht bieten, werden zukünftig Schwierigkeiten haben, Mitarbeiter zu einer Entsendung zu motivieren bzw. überhaupt für Fachkräfte am Arbeitsmarkt attraktiv zu sein. Die Hinterbliebenenabsicherung kann in der Unfallversicherung durch ein einmaliges Sterbegeld in beliebiger Höhe erfolgen.

Speziell für die Unfallversicherung von entsandten Mitarbeitern gelten analog zur Krankenversicherung (vgl. Abschn. 30.2.3) auch besondere Serviceleistungen, wie zum Beispiel eine 24-Stunden Hotline, die bei der Auswahl von Fachärzten im Ausland beraten kann.

Weiterhin zu beachten sind die speziellen Meldefristen in der Unfallversicherung. Diese können von Versicherer zu Versicherer variieren und sind dem jeweiligen Bedingungswerk zu entnehmen. Grundsätzlich muss jeder eingetretene Unfall unverzüglich beim Versicherer gemeldet werden. Insbesondere bei Invaliditätsleistungen gelten besondere Fristen. Die Invalidität muss innerhalb eines gewissen Zeitraums nach dem Unfall eintreten und innerhalb einer weiteren Frist ärztlich festgestellt und geltend gemacht werden (vgl. GDV 2014, S. 5). Die Einhaltung dieser Fristen ist unabdingbar. Auch wenn der Arbeitnehmer durch einen Unfall unstrittig nachhaltig geschädigt wurde, könnte der Versicherer die Leistungen verweigern, falls die Meldefristen nicht eingehalten wurden. Dies wurde bereits mehrfach durch Gerichtsurteile gestützt (vgl. OLG Karlsruhe, Urteil vom 07.09.2000 – 12 U 122/00 oder OLG Karlsruhe 03.05.2005 – 12 U 290/04).

Auch die Unfallversicherung enthält Ausschlüsse, die den Versicherungsschutz einschränken. So gilt zum Beispiel der Kriegsausschluss ebenso wie in der Krankenversicherung (vgl. Abschn. 30.2.3).

Ein weiteres Risiko, das der Arbeitgeber beim Travel Risk Management berücksichtigen sollte, ist die Kriminalität im Ausland. Der Fokus des folgenden Abschnitts liegt auf der Entführungsgefahr, denn Entführungen sind ein aktuelles Thema und eine Gefahr, die häufig unterschätzt wird.

30.4 Kriminalität

30.4.1 Gefahren

Neben den oben beschriebenen Gefahren durch Krankheiten oder Unfälle stellt die Kriminalität eine weitere Gefahr für entsandte Mitarbeiter dar. In Krisenregionen oder Ländern mit hoher Kriminalitätsrate sind diesbezüglich besondere Vorsichtsmaßnahmen geboten. Das Spektrum der Gefahren, denen die Mitarbeiter unter Umständen ausgesetzt sein können, kann von Diebstahl bis zur Entführung oder sogar Mord gehen. Insbesondere die Anzahl von Entführungen ist in den vergangenen Jahren signifikant angestiegen. Da für Entführungsfälle mittlerweile spezielle Versicherungslösungen existieren, soll diese Gefahr im Fokus dieses Abschnitts stehen.

Eichel und Sauer, Geschäftsführer und Inhaber des Sicherheitsunternehmens Result Group, geben an, dass jedes Jahr ca. 10.000 Entführungen weltweit offiziell gemeldet werden. Sie gehen jedoch davon aus, dass die Dunkelziffer weitaus höher ist. Es wird vermutet, dass weltweit nur zehn Prozent der Entführungen gemeldet werden. Dies geschieht in erster Linie zum Schutz des Opfers, da Entführer meist die Bedingung stellen, keine Behörden einzuschalten (vgl. Eichel et al. 2018, S. 17 f.).

Zudem treten vermehrt sogenannte Expressentführungen auf. Diese sind dadurch gekennzeichnet, dass sie nur wenige Stunden andauern und mit der Forderung geringer Lösegeldsummen verbunden sind. Aufgrund der kurzen Entführungsduer und des vergleichbar geringen finanziellen Schadens werden diese häufig nicht gemeldet (vgl. Eichel et al. 2018, S. 17 f.). Ein klassischer Fall für eine Expressentführung ist zum Beispiel folgendes Szenario: In der Nacht steigt der Reisende nach Ankunft am Flughafen in einem fremden Land in ein vermeintliches Taxi. Der Fahrer fordert den Reisenden unter Androhung von Gewalt auf, das Tageslimit seiner Kreditkarte vom Geldautomaten abzuheben. Am folgenden Tag wird erneut gefordert, das Tageslimit abzuheben, und im Anschluss wird die Geisel freigelassen.

Die Hochrisikogebiete für Entführungen befinden sich im afrikanischen und mittel- bzw. südamerikanischen Raum. Besonders hervorzuheben sind hier Staaten wie Mexiko, Somalia oder Libyen. Die Result Group, die auch als Krisenberater mit Versicherern zusammenarbeitet, veröffentlicht auf ihrer Website jährlich eine aktualisierte Version der „World Threat Map“. Vergleicht man die Risikolandkarten der letzten vier Jahre, fällt auf, dass sich insbesondere die Sicherheitslage in Afrika signifikant verschlechtert hat. Dabei spielen vor allem Terror, Bürgerkriege und Korruption eine große Rolle. Weitere Krisengebiete mit hohem Entführungspotenzial sind Teile Nordafrikas und des Nahen Ostens. Radikal islamistische Gruppierungen nutzen die Lösegelder aus Entführungen, um Waffen zu kaufen. Weiterhin ist der religiöse Konflikt zwischen Schiiten und Sunniten besonders relevant für die Krisen in dieser Region. In den gefährdeten Regionen Mittelamerikas bzw. Südamerikas sind insbesondere Armut, Chancengleichheit und Korruption Gründe für die steigende Kriminalität (vgl. Trauboth et al. 2016, S. 268 f.).

Wie bereits erwähnt steigt die Anzahl der Entführungen kontinuierlich an und das Problem weitet sich aus. Neben den Krisenherden in Afrika und Südamerika, in denen die Entführungsproblematik bereits bekannt ist, werden auch aus weiten Teilen Osteuropas immer mehr Entführungen gemeldet. Zudem nimmt die Brutalität der Entführer zu und es häufen sich Entführungsfälle, in denen Geiseln verletzt oder getötet werden. Ebenfalls verlängert sich der zeitliche Rahmen von Entführungen. Eine durchschnittliche Entführung in der heutigen Zeit dauert ca. elf Monate (vgl. Bundesnachrichtendienst 2018). Im folgenden Abschnitt wird aufgezeigt, wie man seine Mitarbeiter auf eine Entsendung in ein Krisengebiet vorbereitet, um so das Entführungsrisiko zu minimieren.

30.4.2 Präventionsmaßnahmen

Genau wie bei dem Schutz vor Krankheiten oder Unfällen ist eine umfangreiche Vorbereitung des Arbeitnehmers die Basis für den Schutz vor Kriminalität, insbesondere vor Entführungen. Idealerweise erfolgt diese Vorbereitung nicht durch den Arbeitgeber selbst, sondern durch private Sicherheitsunternehmen, die sich auf den Umgang mit Krisensituationen spezialisiert haben. Man spricht in dem Zusammenhang von sogenannten Krisenberatern. Diese sind Experten in der Prävention von Entführungen, aber auch im Umgang mit Verhandlungen und Lösegeldübergaben. Die Mitarbeiter sind nicht selten ehemalige Polizisten oder Soldaten. Zudem sind die Krisenberater, auch in Bezug auf Behörden, sehr gut vernetzt (vgl. Trauboth et al. 2016, S. 293).

Die zentrale Aufgabe eines Krisenberaters ist die Erstellung eines ganzheitlichen Sicherheitskonzeptes. Die Mitarbeiter erhalten Informationen über die Gesetze des jeweiligen Landes, die Sicherheit am Einsatzort und zu Verhaltensweisen im Entführungsfall. Zudem finden sprachliche und medizinische Vorbereitungsmaßnahmen statt. Meistens erfolgt eine Eintragung in die Krisenvorsorgeliste des Auswärtigen Amtes. Dies ist ein Verzeichnis, in dem deutsche Staatsbürger, die sich im Ausland befinden, aufgeführt sind. Im Ernstfall erleichtert dies eine Kommunikation mit allen Beteiligten. Eine der wichtigsten Aufgaben des Sicherheitskonzeptes ist die Errichtung des Krisenstabes. Dies ist eine Organisationseinheit im jeweiligen Unternehmen, die speziell zur Lösung einer Krise, einberufen wird. Die Mitglieder des Krisenstabes treffen unter Zeitdruck Entscheidungen, die weitreichende Konsequenzen nach sich ziehen. Daher müssen die Krisenstabsmitglieder sorgfältig auf ihre Eignung geprüft werden (vgl. Trauboth et al. 2016, S. 459).

Es wird genau festgehalten, wer im Schadenfall welche Aufgabe hat und wer zu welcher Zeit informiert wird. Die Abgrenzung der Kompetenzen und der Entscheidungsbefugnisse sind besonders wichtig, damit im Entführungsfall ein reibungsloser Ablauf der Maßnahmen stattfindet. Wichtige Positionen, die im Krisenstab besetzt werden, sind unter anderem der Leiter des Krisenstabes, eine Person, die die Kommunikation mit der Polizei, dem Krisenberater und dem Versicherer übernimmt, und ein Rechtsexperte (vgl. Trauboth et al. 2016, S. 299 f.).

Zudem werden Richtlinien festgelegt, wie sich Mitarbeiter, die ins Ausland entsendet werden, verhalten sollen. Wichtig ist dies insbesondere in Ländern, in denen die Behörden stark korrumptiert und in denen einzelne Beamte unter Umständen an Entführungen beteiligt sind (vgl. Schneider 2003, S. 133, 276).

Die Tagessätze von Krisenberatern inkl. Spesen liegen häufig im mittleren vierstelligen Bereich. Daher empfiehlt sich der Abschluss einer sogenannten Kidnap & Ransom Versicherung (K&R Versicherung). Dies ist der englische Fachbegriff für die Entführungs- und Lösegeldversicherung. Diese Versicherung deckt unter anderem auch die Kosten für Präventionsmaßnahmen durch spezialisierte Krisenberater. Im folgenden Abschnitt werden die einzelnen Komponenten der K&R Versicherung näher erläutert.

30.4.3 Versicherungslösungen

Grundlage der folgenden Ausführungen sind drei, nicht veröffentlichte Versicherungsbedingungen von Anbietern der K&R Versicherung. Zentraler Bestandteil der K&R Versicherung ist die Erstattung eines Lösegeldes im Falle einer Entführung. Nachdem ein gefordertes Lösegeld an die Entführer übergeben wurde, erstattet der Versicherer dieses. Hierbei gilt es zu beachten, dass das versicherte Unternehmen in Vorleistung gehen muss. Dies hat den Hintergrund, dass der Versicherer nur ein Lösegeld zahlt, welches das versicherte Unternehmen auch selbst hätte finanzieren können. Diese Vorgehensweise deckt sich mit den Richtlinien des damaligen Bundesaufsichtsamts für Versicherungswesen (BAV), das heute unter dem Namen Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) die Versicherer beaufsichtigt. Aus einem Rundschreiben von März 1998, welches bis heute Bestand hat, geht hervor, dass die Versicherungssumme den wirtschaftlichen Verhältnissen des Versicherungsnehmers entsprechen muss (vgl. Bundesaufsichtsamt für Versicherungswesen 1998). So soll das moralische Risiko gesenkt und dem Versicherungsbezug entgegengewirkt werden.

Der Versicherer zahlt kein Lösegeld direkt an den Entführer, sondern nur an das Unternehmen. Zudem leistet der Versicherer auch, wenn das Lösegeld während des Transports auf dem Weg zur Übergabe abhandenkommt. Voraussetzung hierfür ist, dass den Weisungen des Täters Folge geleistet wird und der Transport durch eine Person erfolgt, die in Abstimmung mit dem Versicherer ausgesucht wird. Ist der Versicherer nicht davon überzeugt, dass der ausgewählte Überbringer dazu in der Lage ist, das Lösegeld sicher zu überbringen, kann er vorgeben, dass eine andere Person mit der Überbringung beauftragt wird. Für ein solches Szenario bietet sich ein Mitarbeiter des Krisenberaters an. Häufig wird jedoch eine Person durch den Täter bestimmt. Sollte das Lösegeld verloren gehen, ohne dass das Unternehmen Absprache mit dem Versicherer getroffen hat, ist dieser Verlust nicht gedeckt. Es ist definitiv ratsam, den Überbringer des Lösegeldes mit dem Versicherer abzustimmen, da eine Übergabe ein unvorhersehbares Ereignis ist, bei dem ein Verlust nicht unwahrscheinlich ist (vgl. Schneider 2003, S. 130).

Falls das versicherte Unternehmen einen Kredit aufnehmen muss, um das Lösegeld vorzustrecken, werden anfallende Darlehenszinsen ebenso vom Versicherer übernommen. Hierbei gilt jedoch die Geheimhaltungsobliegenheit. Erzählt das Unternehmen dem Kreditinstitut bei der Aufnahme des Kredits von der Lösegeldversicherung, verletzt er die Geheimhaltungsobliegenheit und der Versicherer könnte unter Umständen leistungsfrei sein. Es ist sehr wichtig, dass der Abschluss einer solchen Police strengster Geheimhaltung unterliegt. Somit soll gewährleistet sein, dass potenzielle Entführer nicht in Erfahrung bringen können, welche Unternehmen sich gegen Entführungen ihrer Mitarbeiter haben absichern lassen.

Neben der Erstattung des Lösegeldes sind noch zahlreiche weitere versicherte Schäden und Kosten Bestandteil der Police. Wie oben bereits erwähnt, werden auch die Kosten für einen Krisenberater erstattet. Hierbei handelt es sich sowohl um die Kosten für die Präventionsmaßnahmen als auch um Kosten im Entführungsfall, wenn Lösegeldverhandlungen oder -übergaben erforderlich sind. Faktisch ist der Einkauf einer K&R Versicherung als Komplettpaket verhältnismäßig günstiger als die selbstständige Beauftragung eines Krisenberaters durch das Unternehmen. Die Versicherer stehen bzgl. der Gagen der Krisenberater in einer besseren Verhandlungsposition als ein einzelnes Unternehmen und haben Rahmenverträge mit vielen etablierten Krisenberatern geschlossen (vgl. Schneider 2003, S. 134 f.).

Wie bereits in Abschn. 30.1.1 näher erläutert, kann der Arbeitnehmer Schadenersatzansprüche gegenüber seinem Arbeitgeber geltend machen, sollte dieser seinen Fürsorgepflichten nicht nachgekommen sein. Erhebt eine versicherte Person aufgrund einer Entführung oder Erpressung Klage gegen das Unternehmen und wird dieser daraufhin zur Zahlung von Schadenersatz verurteilt, leistet der Versicherer. Häufig ist auch die Abwehr von unberechtigten Schadenersatzansprüchen Teil der K&R Versicherung.

Kosten für medizinische Aufwendungen von versicherten Personen sind als Folge einer Entführung in mehrfacher Hinsicht versichert. Zum einen sind die Kosten für kosmetische und plastische Operationen versichert, falls eine versicherte Person als Folge eines versicherten Ereignisses dauerhaft entstellt wird. Ebenso werden die Kosten für Genesungs- und Rehabilitationsmaßnahmen für eine gewisse Dauer nach der Freilassung der entführten Person erstattet. Weiterhin sind Invalidität oder Tod als Folge eines Unfalls versichert. Voraussetzung für das Vorliegen eines Unfalls sind die gleichen Merkmale wie in der klassischen Unfallversicherung: ein plötzlich von außen auf den Körper einwirkendes Ereignis, welches zu einer unfreiwilligen Gesundheitsschädigung führt. Der Unfall muss die unmittelbare Folge der Entführung sein und die Invalidität oder der Tod muss binnen zwölf Monaten nach dem Unfall eintreten. Neben den Kosten, die durch körperliche Schäden verursacht werden, erfolgt auch eine Erstattung für Kosten durch psychologische und psychiatrische Betreuung. Insbesondere Entführungen oder Geiselnahmen sind Ereignisse, die für die Opfer und Angehörigen traumatische Folgen haben können. In vielen Fällen überwiegt der psychische Schaden sogar dem körperlichen Schaden (vgl. Dahms und Völker 2016, S. 189 ff.). Honorare für eine solche Behandlung werden den versicherten

Personen bis maximal 24 Monate nach dem Versicherungsfall bzw. maximal 24 Monate nach der Freilassung des Entführungsopfers vom Versicherer bezahlt.

Bei der Befreiung eines entführten Mitarbeiters können weitere Kosten anfallen. Dazu zählen zum Beispiel die Kosten für einen Unterhändler oder einen Dolmetscher. In manchen Krisengebieten ist es erforderlich, Unterhändler vor Ort einzuschalten, da sie die örtlichen Gegebenheiten und die Motive der Täter besser einschätzen können als die Krisenberater. Sie bilden eine gute Ergänzung zum Einsatz der Krisenberater. Falls erforderlich, erstattet der Versicherer auch die Kosten des Aussetzens einer Belohnung für das Ergreifen der Täter. Der Versicherer entscheidet in diesen Fällen, in Absprache mit dem Krisenberater, über die Angemessenheit dieser Maßnahmen. Falls weitere technische Ausrüstungen erforderlich sind (zum Beispiel Kommunikationsmittel), übernimmt der Versicherer auch hierfür die Kosten. Weiterhin werden Aufwendungen für Wachpersonal erstattet, welches die Sicherheit weiterer Personen gewährleisten soll. Das ist zum Beispiel der Fall, wenn die Familie des Entführten diesen ins Ausland begleitet hat und darauffolgend die Gefahr besteht, dass die Angehörigen ebenfalls entführt werden. Sofern weitere Aufwendungen notwendig sind, um das Entführungsopfer zu befreien, werden diese ebenso erstattet. Der Versicherer muss jedoch dafür vorher sein Einverständnis geben.

Das oberste Ziel der Lösegeldversicherung ist zwar die Befreiung der versicherten Personen, jedoch geht der Versicherungsschutz weit darüber hinaus. Ein weiterer Bestandteil ist es, die finanzielle Schlechterstellung der versicherten Mitarbeiter und des Arbeitgebers im Versicherungsfall zu verhindern. Daher werden die aus dem Versicherungsfall entstehenden persönlichen Vermögensschäden der versicherten Personen erstattet. Zudem sind sowohl die Weiterzahlung des Bruttogehaltes des entführten Mitarbeiters als auch Aufwendungen und Gehälter für weitere Angestellte, die bei der Freilassung der Geisel in jeglicher Form helfen, in der K&R Versicherung gedeckt. Einige Versicherer erstatten ergänzend noch Kosten für einen externen Public Relation Berater, der die Öffentlichkeitsarbeit übernimmt.

30.5 Fazit

Im ersten Abschnitt wurde die Haftungsfrage des Arbeitgebers anhand seiner gesetzlichen Fürsorgepflichten analysiert. Insbesondere das Zielland der Entsendung ist dabei von Relevanz. Je mehr sich das Zielland hinsichtlich Versorgung, Kultur und Sicherheitsstandards unterscheidet, desto umfangreicher sollten die Vorbereitungsmaßnahmen sein. Zudem ist hervorzuheben, dass das Unternehmen ein originäres Interesse an dem Wohlergehen des Mitarbeiters während einer Entsendung hat. So muss es zum Beispiel bei einer Krankheit des entsandten Mitarbeiters mit Umsatzeinbußen oder dem Verlust von Geschäftsbeziehungen rechnen. Des Weiteren werden Aspekte wie „Corporate Social Responsibility“ und „Employer Branding“ zunehmend relevanter und sind in die Management-Prozesse zu implementieren. Fachkräfte sind auf dem Arbeitsmarkt hart umkämpft. Sie erwarten entsprechende Bemühungen ihres Arbeitgebers und eine angemessene finanzielle und

gesundheitliche Absicherung (insbesondere in Situationen wie Entsendungen). Sollte ein Arbeitgeber dies nicht erbringen, wird es schwierig werden, qualifiziertes Personal für sein Unternehmen zu gewinnen.

Aufgrund schlechterer Hygienestandards oder der Verbreitung von Infektionskrankheiten ist der Mitarbeiter einem Gesundheitsrisiko ausgesetzt, das er aus Deutschland in dem Ausmaß nicht kennt. Daher sollte vor der Entsendung eine Beratung und Behandlung durch Fachärzte erfolgen. Neben der körperlichen Gesundheit gilt es, auch die psychische Gesundheit des Mitarbeiters zu schützen. Dieser könnte ggf. einen Kulturschock erleiden. Um dem vorzubeugen, sollte der Mitarbeiter mittels eines interkulturellen Trainings auf die neue Umgebung vorbereitet werden. Da der Arbeitgeber für die medizinische Behandlung des entsandten Mitarbeiters und mitreisender Familienangehöriger finanziell aufkommen muss, empfiehlt sich der Abschluss einer internationalen Krankenversicherung. Diesbezüglich ist es von Vorteil, wenn der Versicherer über ein internationales Netzwerk verfügt und umfangreiche Assistance-Leistungen anbietet, wie zum Beispiel durch mehrsprachige 24-Stunden Hotlines.

Neben dem Krankheitsrisiko existiert in vielen Ländern auch ein erhöhtes Unfallrisiko. Der Mitarbeiter kann sich während der Arbeit durch nicht ausreichend gesicherte Gefahrenstellen oder nicht gewartete Maschinen verletzen. Daher sollte er sorgfältig über den Umgang mit den jeweiligen Werkzeugen und Maschinen unterrichtet werden. Durch geeignete Risk-Management-Maßnahmen sollte weitestgehend sichergestellt werden, dass der entsandte Mitarbeiter unter den gleichen Sicherheitsstandards arbeitet wie an seinem Arbeitsplatz in Deutschland. Da trotzdem in den meisten Fällen eine erhöhte Unfallgefahr herrscht, ist der Abschluss einer Gruppenunfallversicherung für die Mitarbeiter von Seiten des Unternehmens zu empfehlen. Die Leistungen sind individuell wählbar, sollten jedoch ausreichenden finanziellen Schutz im Falle einer Invalidität des Mitarbeiters bieten.

Das Entführungsrisiko ist insbesondere in Krisenländern relevant. Falls Mitarbeiter in solche entsandt werden, ist es notwendig, umfangreiche Vorbereitungsmaßnahmen zu treffen. Diese kann das Unternehmen in der Regel nicht allein durchführen, da hierfür spezielles Know-how erforderlich ist. Krisenberater, die sich auf Entführungen spezialisiert haben, bieten diesen Service an. So führen sie Sicherheitstrainings durch, in denen den Mitarbeitern aufgezeigt wird, durch welche Verhaltensweisen das Entführungsrisiko minimiert werden kann. Zusätzlich wird gelehrt, wie sich die Mitarbeiter bei einer tatsächlichen Entführung verhalten sollen. Zudem bereiten sie auch das Unternehmen auf solche Situationen vor, nämlich durch die Implementierung eines Krisenstabs. Die Kosten hierfür übernimmt die K&R Versicherung ebenso wie die Zahlung eines Lösegeldes im Falle einer Entführung. Die Tatsache, dass ein Unternehmen eine K&R Versicherung abgeschlossen hat, darf unter keinen Umständen nach außen dringen, da potenzielle Entführer sonst einen zusätzlichen Anreiz hätten, sich auf diese Unternehmen zu fokussieren.

Abschließend lässt sich zusammenfassen, dass die Risiken der o. g. Gefahren durch geeignete Präventionsmaßnahmen deutlich minimiert werden können. Hierfür muss ein Travel Risk Management implementiert werden, in dem die Risiken analysiert werden.

Durch passenden Versicherungsschutz werden ergänzend weitere finanzielle Risiken minimiert.

Literatur

- Balme, F., & Ruscheinsky, D. (2017). Gefahren und Risiken bei Auslandsreisen. *VersicherungsPraxis*, 10/17, 13–17.
- Baum, G. (2017). Internationale Krankenversicherung: Rund um die Welt gut abgesichert. *VersicherungsPraxis*, 10/17, 18–20.
- Bereuter-Hämmerle, K. B. (2016). *Leitfaden für internationale Entsendungen und Expatriate-Management*. Mittweida: University of Applied Sciences, Wirtschaftswissenschaftliche Fakultät.
- Bundesanstalt für Arbeitsschutz und Arbeitsmedizin in Zusammenarbeit mit dem Bundesministerium für Arbeit und Soziales (BMAS). (2016). Sicherheit und Gesundheit bei der Arbeit 2014 Unfallverhütungsbericht Arbeit. baua.de. https://www.baua.de/DE/Angebote/Publikationen/Beichte/pdf/Suga-2014-barrierefrei.pdf?__blob=publicationFile&v=4. Zugegriffen am 22.04.2019.
- Bundesaufsichtsamt für Versicherungswesen. (1998). Rundschreiben 3/1998 (VA) – Hinweise des BAV zum Betrieb von Lösegeldversicherungen. bafin.de. https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/rs_9803_va_loesegeldversicherung.html. Zugegriffen am 22.04.2019.
- Bundeskommunikationsamt. (2018). Entführungen deutscher Staatsbürger im Ausland. bnd.bund.de. http://www.bnd.bund.de/DE/Themen/Lagebeitraege/Entfuehrungen/Entfuehrungen_node.html. Zugegriffen am 02.04.2019.
- Bungard, P. (2018). *CSR und Geschäftsmodelle – Auf dem Weg zum zeitgemäßen Wirtschaften*. Köln: Springer.
- Dahms, P., & Völker, B. (2016). Psychologische Aspekte bei Geiselnahmen. *Organisationsberatung, Supervision, Coaching*, 23, 189–199.
- Deutsche Gesetzliche Unfallversicherung (DGUV). (2013). Calculating the international return on prevention for companies: Costs and benefits of investments in occupational safety and health. publikationen.dguv.de. https://publikationen.dguv.de/dguv/pdf/10002/23_05_report_2013-en%2D%2D-web-doppelseite.pdf. Zugegriffen am 28.04.2019.
- Eichel, C., et al. (2018). Entführung und Erpressung als Geschäftsmodell. *VersicherungsPraxis*, 03/18, 17–18.
- Fuhlrott, M./Schröder, T. (2017), „Lösegeldzahlungen des Arbeitgebers an terroristische Organisationen aus arbeits- und strafrechtlicher Sicht“. *NZA-Rechtsprechungsreport Arbeitsrecht*, 12, 625–680.
- GDV. (2014). Allgemeine Unfallversicherungsbedingungen AUB 2014 Musterbedingungen des GDV. gdv.de. <https://www.gdv.de/resource/blob/6252/952c52d93fc486c4970a8c33e2ea0d1e/01-allgemeine-unfallversicherungsbedingungen%2D%2Daub-2014%2D%2Ddata.pdf>. Zugegriffen am 09.05.2019.
- Hechler, S. (2015). *Die Entsendung von Führungskräften ins Ausland: Hintergründe – Grundlagen – Empfehlungen*. Hamburg: Bachelor + Master Publishing.
- International SOS Foundation. (2014). *Rechte und Pflichten deutscher Unternehmen gegenüber ihren Arbeitnehmern bei der Auslandentsendung*. Neu-Isenburg: International SOS Foundation.
- International SOS Foundation. (2018). Road accidents & safety. internationalsos.com. <https://www.internationalsos.com/topics/road-accidents>. Zugegriffen am 28.04.2019.
- International SOS Foundation. (2019). *Berufliche Auslandsreisen und Entsendungen: Leitfaden zur Erstellung der Gefährdungsbeurteilung*. Neu-Isenburg: International SOS Foundation.

- Ipsos Institute. (2018). Global views on healthcare – 2018. [Ipsos.com](https://www.ipsos.com/sites/default/files/ct/news/documents/2018-07/global-views-on-healthcare-2018-ipsos-global-advisor.pdf). <https://www.ipsos.com/sites/default/files/ct/news/documents/2018-07/global-views-on-healthcare-2018-ipsos-global-advisor.pdf>. Zugegriffen am 13.04.2019.
- Karlshaus, A., et al. (2019). *CSR und Interkulturelles Management – Gesellschaftliche und unternehmerische Verantwortung international bewältigen*. Berlin: Springer.
- Pfannstiel, M., et al. (2019). *Internationalisierung im Gesundheitswesen*. Wiesbaden: Springer.
- Schneider, G. (2003). *Versicherungsschutz gegen Erpressungen*. Karlsruhe: Versicherungswirtschaft Karlsruhe.
- Trauboth, J. H., et al. (2016). *Krisenmanagement in Unternehmen und öffentlichen Einrichtungen: professionelle Prävention und Reaktion bei sicherheitsrelevanten Bedrohungen von innen und außen* (J. H. Trauboth, Hrsg.). Stuttgart: Richard Boorberg.
- Unfallversicherung – Ausland(DVUA)/Deutsche Gesetzliche Unfallversicherung (DGUV). (2018). Gesetzliche Unfallversicherung bei Entsendung ins Ausland. publikationen.dguv.de. https://publikationen.dguv.de/dguv/pdf/10002/guv_aus.pdf. Zugegriffen am 19.05.2019.
- Verband Deutsches Reisemanagement. (2018). VDR-Geschäftsreiseanalyse 2018. vdr-service. de. https://www.vdr-service.de/fileadmin/services-leistungen/fachmedien/geschaeftsreiseanalyse/VDR-Geschaeftsreiseanalyse-2018_GRA.pdf. Zugegriffen am 06.04.2019.
- World Health Organization. (2018). World malaria report 2018. apps.who.int. <https://apps.who.int/iris/bitstream/handle/10665/275867/9789241565653-eng.pdf?ua=1>. Zugegriffen am 14.04.2019.

Martin Gary startete seine Karriere in der Lufthansa Group 1997 bei der damals noch eigenständigen Austrian Airlines (AUA). Der Jurist verantwortete dort unter anderem als Legal Counsel im Konzernrechtsbüro der AUA den Aufbau einer Antitrust Compliance Einheit. Im Jahr 2003 wurde er dann zum Generalbevollmächtigten des hauseigenen Versicherungsmaklers AUA Versicherungs-Service GesmbH ernannt. Ab November 2007 verantwortete er als Abteilungsleiter Konzernversicherungen die gesamte Absicherung und das Risikomanagement der Austrian Airlines Group. Im Januar 2018 wechselte Gary als Generalbevollmächtigter zur Albatros Versicherungsdienste GmbH, wo er zum 01. November 2018 zum Mitglied der Geschäftsführung berufen wurde.

Tim Thomas beendete im Jahr 2015 seine Berufsausbildung zum Kaufmann für Versicherungen und Finanzen bei der Signal Iduna Gruppe. Im Anschluss studierte er Versicherungswesen mit den Schwerpunkten Sach- und Betriebsunterbrechungsversicherungen, Haftpflichtversicherung und Personalmanagement am Institut für Versicherungswesen der Technischen Hochschule Köln. Darauf aufbauend absolvierte er dort auch das Masterstudium Risk & Insurance. Während des Studiums arbeitete er im Underwriting bei dem amerikanischen Industriever sicherer CNA Hardy.



Betriebliche Altersversorgung

31

Ingo Trosiner und Dominik Hartmann

Zusammenfassung

In diesem Kapitel wird ein kurzer, kompakter Überblick über die wesentlichen Kernpunkte der betrieblichen Altersversorgung gegeben. Der Fokus liegt dabei auf den rechtlichen Fragestellungen und wichtigen Punkten, die in der Praxis gelegentlich nicht beachtet werden und somit aus Arbeitgebersicht unerwünschte Probleme mit sich bringen können. Die betriebliche Altersversorgung stellt eine immer wichtiger werden Rolle im Versorgungssystem der zukünftigen Rentner dar. Auf diese Rolle wird zur besseren Einordnung zu Beginn des Kapitels eingegangen. Das durch die Bundesregierung beschlossene und zum Jahresbeginn 2018 in Kraft getretene Betriebsrentenstärkungsgesetz wird in diesem Kapitel ebenfalls aufgegriffen und die hiermit zusammenhängenden, wichtigsten Neuerungen und Fragestellungen näher beleuchtet.

31.1 Einführung und Einordnung der betrieblichen Altersversorgung

31.1.1 Versorgungssituation in Deutschland

Versicherte, die bereits eine Renteninformation der Deutschen Rentenversicherung erhalten haben, lesen in ihrem Schreiben, dass „die Renten im Vergleich zu den Löhnen künftig

I. Trosiner
comdirect Versicherungsmakler AG, Quickborn, Deutschland
E-Mail: Ingo.trosiner@mein.comdirect-versicherungsmakler.de

D. Hartmann (✉)
TH Köln, Institut für Versicherungswesen, Köln, Deutschland
E-Mail: dominik.hartmann@posteo.de

geringer steigen werden und sich somit die spätere Lücke zwischen Rente und Erwerbs-einkommen vergrößert [...]“ (Deutsche Rentenversicherung Bund 2019, S. 24).

Die sich hieraus ergebende Folge ist, dass Personen, die mit Arbeitseinkommen ihren Lebensunterhalt bestreiten, bei Fortfall dieser Zahlungen teils erhebliche finanzielle Einbußen hinnehmen müssen. Um diese Einbußen zu kompensieren, sollten ergänzende Einnahmequellen aufgebaut werden. Dies kann auf unterschiedlichen Wegen erfolgen. Eine der Möglichkeiten stellt die betriebliche Altersversorgung (bAV) dar. Durch diese Art der Vorsorge können zusätzlich zur gesetzlichen Rente nach Rentenbeginn zusätzliche Einnahmen generiert werden.

Nach den Rentenreformen 2001 und der damit verbundenen Stärkung der kapitaldeckten Altersversorgung bei gleichzeitiger Absenkung des Rentenniveaus wurde die Bevölkerung stärker in die Verantwortung genommen. Neben dieser Absenkung des Rentenniveaus der gesetzlichen Rentenversicherung sind weitere Gründe für die Bedürftigkeit im Alter „Erwerbsbiografien mit längerfristig niedrigen Einkommen (auch durch Teilzeit) und längeren Arbeitsunterbrechungen durch Arbeitslosigkeit oder aus anderen Gründen“ (Bundesministerium für Arbeit und Soziales 2016a, S. 11).

Es gibt neben der bAV eine Vielzahl von Vorsorgemöglichkeiten, aus denen gewählt werden kann. Heute ist es aber auch durch eben diese Vielzahl an Möglichkeiten deutlich komplexer geworden, privat vorzusorgen, denn die Zeiten, in denen die gesetzliche Rente kombiniert mit einer gut verzinsten privaten Rentenversicherung den Lebensstandard sichern konnte, sind vorbei. Die laufende Verzinsung deutscher Lebensversicherungsverträge hat sich innerhalb der letzten 20 Jahre, seit dem Jahr 1999, drastisch reduziert. So konnte sich ein Versicherungsnehmer einer klassischen Rentenversicherung im Jahr 1999 noch über eine laufende Verzinsung von mehr als sieben Prozent freuen (vgl. Assekurata 2016, S. 9), wohingegen sich Versicherungsnehmer im Neugeschäft 2019 mit etwa 2,5 Prozent begnügen müssen (vgl. Assekurata 2019, S. 2).

Die Verbreitung der bAV hängt häufig unmittelbar mit der Größe des jeweiligen Betriebes zusammen. So zeigt das Bundesministerium für Arbeit und Soziales im Alterssicherungsbericht 2016, dass in Betrieben mit 1000 und mehr Mitarbeitern statistisch etwa 83 Prozent der Arbeitnehmer eine bAV haben, wohingegen in kleinen Betrieben die Verbreitung deutlich abnimmt, wie man im Folgenden sehen kann (vgl. Tab. 31.1).

Tab. 31.1 Verbreitung betrieblicher Altersversorgung nach Betriebsgröße. (Quelle: Bundesministerium für Arbeit und Soziales 2016b, S. 136)

Beschäftigte	Anteil der Beschäftigten mit bAV
1000 und mehr	83 %
500 bis 999	65 %
250 bis 499	58 %
50 bis 249	44 %
10 bis 49	38 %
1 bis 9	28 %

31.1.2 Drei-Schichten-Modell

Für große Teile der deutschen Bevölkerung stellt die gesetzliche Rentenversicherung einen wichtigen Bestandteil der Alterseinkünfte dar. Rund drei Viertel der Einnahmen im Alter stammen aus Rentenzahlungen der Deutschen Rentenversicherung (vgl. Bundesministerium für Arbeit und Soziales 2016, S. 93). Wie schon aufgezeigt reichen die gesetzlichen Alterssicherungssysteme nicht mehr aus, um den gewünschten Lebensstandard zu halten. Deswegen wurden zusätzlich zur umlagefinanzierten gesetzlichen Rentenversicherung kapitalgedeckte Alterssicherungssysteme, wie die bAV und die im Volksmund auch „Riesterrente“ und „Rüruprente“ genannten Alterssicherungssysteme, etabliert. Einander ergänzend können Umlageverfahren und die kapitalgedeckten Alterssicherungssysteme so den Lebensstandard der zukünftigen Rentner erhöhen. Gleichzeitig entsteht auf dieses Weise eine Risikostreuung, da aus verschiedenen Alterssicherungssystemen ein Alterseinkommen gezahlt wird.

Abb. 31.1 bietet einen Überblick über den Aufbau des Drei-Schichten-Modells und zeigt, für welche Personengruppen die jeweiligen Alterssicherungssysteme in Frage kommen.

Die Basis in der 1. Schicht stellen die gesetzlichen Sicherungssysteme dar, wie die gesetzliche Rentenversicherung, die berufsständischen Versorgungswerke und die Beamtenversorgung. Die „Rüruprente“ befindet sich ebenfalls in Schicht 1 und kann von jeder Perso-

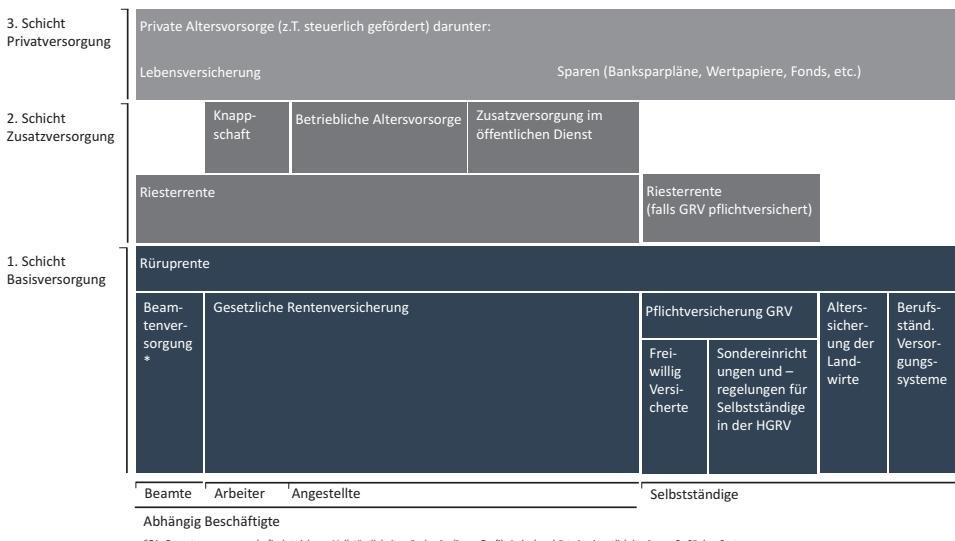


Abb. 31.1 Aufbau des Drei-Schichten-Modells. (Quelle: eigene Darstellung in Anlehnung an Bundeszentrale für politische Bildung 2019)

nengruppe freiwillig abgeschlossen werden. Sie dient vorwiegend als Ersatz, falls Personen in keinem sozialen Sicherungssystem Mitglied sind, wie zum Beispiel bestimmte Selbstständige, oder zusätzlich etwas für die Altersversorgung steuerbegünstigt einzahlen möchten.

Die 2. Schicht besteht aus der Zusatzversorgung. Hier ist die bAV einzuordnen, da diese eine zusätzliche Alterssicherung darstellt. Ebenso in der 2. Schicht ist die „Riesterrente“ einzuordnen. Bei dieser Vorsorgeform können Förderberechtigte vier Prozent ihres (rentenversicherungspflichtigen) Vorjahresbruttoeinkommens, maximal jedoch 2100 Euro p.a., in einen Riestervertrag einzahlen und die Altersvorsorgebeiträge als Sonderausgaben steuerlich geltend machen.

Unmittelbar förderberechtigt sind Personen, die in der gesetzlichen Rentenversicherung Pflichtbeiträge leisten, Beamte, Richter, Soldaten, Bezieher von ALG I und II, Bezieher einer vollen Erwerbsminderungsrente, Elternteile in Elternzeit, Teilnehmer am Bundesfreiwilligendienst und nicht förderberechtigte Ehepartner von Förderberechtigten mittelbar über diesen.

Riestersparer erhalten zudem sogenannte Zulagen, die in den Riestervertrag fließen. Ebenfalls in der 2. Schicht ist die Zusatzversorgung des öffentlichen Dienstes einzuordnen. In der 3. Schicht kann jegliche Form des Sparens für den Zweck der Privaten Altersvorsorge eingruppiert werden. Insbesondere sind dies Lebens- und Rentenversicherungen, Immobilien, Investmentfonds, Sparverträge und Sparkonten sowie Wertpapiere, wie zum Beispiel Aktien und Anleihen.

31.2 Grundlagen der betrieblichen Altersversorgung

Unter betrieblicher Altersversorgung versteht man „Leistungen der Alters-, Invaliditäts- oder Hinterbliebenenversorgung aus Anlass seines Arbeitsverhältnisses“, die der Arbeitgeber dem Arbeitnehmer zusagt (§ 1 BetrAVG).

31.2.1 Vorteile aus Arbeitgebersicht

Landläufig wird häufig von einer Pflicht des Arbeitgebers gesprochen, seinen Mitarbeitern eine bAV anzubieten. Dies bezieht sich im engeren Sinne aber lediglich auf die Bruttoentgeltumwandlung. Die Grundlage hierfür ist § 1a BetrAVG. Hier wird definiert, dass ein Arbeitnehmer vom Arbeitgeber verlangen kann, dass von seinen künftigen Entgeltansprüchen bis zu vier von Hundert der jeweiligen Beitragsbemessungsgrenze in der gesetzlichen Rentenversicherung durch Entgeltumwandlung für seine betriebliche Altersversorgung verwendet werden.

Welcher Durchführungsweg dabei genutzt wird, entscheidet dabei der Arbeitgeber.

Bietet der Arbeitgeber aktiv keinen Durchführungsweg an, kann der Arbeitnehmer die Bruttoentgeltumwandlung im Rahmen der Direktversicherung verlangen.

Das Recht des Arbeitnehmers ist zugleich eine Pflicht des Arbeitgebers. „Pflicht“ ist im deutschen Sprachgebrauch im Grunde negativ belegt. Bei der bAV aber oftmals ohne Grund. Denn das aktive Anbieten einer bAV – sei es, um dem Recht des Arbeitnehmers auf Bruttoentgeltumwandlung nachzukommen, oder um eine freiwillige arbeitnehmerfinanzierte Lösung anzubieten – beinhaltet einige Vorteile für den Arbeitgeber.

Unternehmen in Deutschland sind sich oft ihrer sozialen Verantwortung und somit ihrer besonderen Fürsorgepflicht bewusst. Dennoch ist die bAV nicht nur ein „bloßes Geschenk“ an die Mitarbeiter, sondern strategisch eingesetzt ist sie ein wichtiges Instrument für die Rekrutierung und Bindung von Mitarbeitern. Vielfach wird ja auf dem Arbeitsmarkt von einem „War for Talents“ gesprochen.

31.2.1.1 Attraktivität auf dem Arbeitsmarkt/Neueinstellung

Die Art und die Höhe der vom Arbeitgeber angebotenen bAV stellt für viele Arbeitnehmer ein wichtiges Kriterium für die Wahl des Arbeitsplatzes dar. Gerade kleinere Unternehmen müssen sich insbesondere bei gut ausgebildeten Fachkräften gegenüber größeren Betrieben behaupten. Da bei Großbetrieben oder Konzernen eine umfangreiche Versorgungsleistung zur Verfügung steht, müssen sich auch kleine Unternehmen im Bereich der bAV engagieren (vgl. Buttler und Keller 2017, S. 15).

„Was wünschen sich die Deutschen von ihrer Arbeit“ untersuchte das infas Institut im Auftrag der ZEIT im Dezember 2018. Neben einem „sicheren Arbeitsplatz“ und „Chefs, die einen weiterentwickeln,“ rangiert die bAV hiernach im ersten Drittel. Nahezu 70 Prozent aller Befragten erachten dieses Thema als sehr wichtig. Demnach ist die bAV wichtiger als persönliche Weiterbildungsmaßnahmen oder der Ruf der Branche (vgl. Müller-Wirth 2018).

31.2.1.2 Bindung der Mitarbeiter

Wenn ein Mitarbeiter das Unternehmen verlässt und somit die Stelle neu besetzt werden muss, entstehen unterschiedliche Kosten, so zum Beispiel durch Rekrutierung, Vertretung etc. Eine attraktive bAV kann die Bindung der Mitarbeiter positiv beeinflussen und hilft daher, die fluktuationsbedingten Kosten zu reduzieren. Bei einer rein arbeitgeberfinanzierten bAV befürchtet der Arbeitgeber, dass er auch dann Aufwände hat, wenn der Mitarbeiter ihn schon nach kurzer Betriebszugehörigkeit wieder verlässt. Diese Furcht ist – zumindest in den ersten Jahren – unbegründet. Scheidet zukünftig ein neuer Mitarbeiter (betrifft Mitarbeiter, die seit dem 01.01.2018 eingestellt wurden) in den ersten drei Beschäftigungsjahren wieder aus, hat er noch keine Ansprüche auf Versorgungsleistungen erwirkt. Die Grundlage ist die sogenannte „Unverfallbarkeit“ der Ansprüche, die erst nach drei Jahren eintritt. Die gesetzliche Grundlage hierfür findet sich in § 1b BetrAVG.

„Unverfallbar“ bedeutet, dass der Arbeitnehmer einen Rechtsanspruch auf das Versorgungsversprechen erhält, obwohl er das Unternehmen verlässt. Verlässt der Mitarbeiter in den ersten drei Jahren das Unternehmen, sind seine Ansprüche noch nicht „unverfallbar“.

31.2.1.3 Verringerung der Lohnnebenkosten

Egal ob es sich um eine arbeitgeber-, oder arbeitnehmerfinanzierte bAV handelt: Der Arbeitgeber kann Lohnnebenkosten in Form von Sozialversicherungsbeiträgen sparen, wenn der jeweilige Mitarbeiter ein Einkommen unterhalb der entsprechenden Beitragsbemessungsgrenze (BBG) bezieht. Die Beiträge sind grundsätzlich bis zu vier Prozent der BBG (West) sozialversicherungsfrei (2020: 3312 Euro p.a.; 276 Euro monatlich). Die Sozialversicherungsfreiheit ergibt sich aus § 3 Nr. 63 EStG in Verbindung mit § 1 Abs. 1 S. 1 Nr. 9 SvEV. Seit Einführung des Betriebsrentenstärkungsgesetzes (BRSG) muss der Arbeitgeber jedoch einen Zuschuss zahlen, soweit er Sozialversicherungsbeiträge einspart.

Bei der Unterstützungskasse und der Direktzusage hängt die Höhe der Sozialversicherungsfreiheit von der Finanzierung ab (Tab. 31.2).

31.2.1.4 Steuerliche Behandlung beim Arbeitgeber

Bei einer arbeitgeberfinanzierten bAV mindern die Beiträge als Betriebsausgabe grundsätzlich in voller Höhe den zu versteuernden Gewinn des Unternehmens. Bei aus Entgeltumwandlung finanzierten Verträgen wird lediglich auf der Betriebsausgabenseite ein Tausch vorgenommen: Anstatt des Lohns/Gehaltes wird ein Versicherungs-/Vorsorgebeitrag gezahlt.

Die genauen Einzelheiten richten sich nach dem gewählten Durchführungsweg. Die Rechtsgrundlagen sind:

- Direktversicherung in § 4 b EStG
- Pensionskasse in § 4 c EStG
- Pensionsfonds in § 4 e EStG
- Unterstützungskasse, § 4 d EStG
- Direktzusage, § 6 a EStG

Tab. 31.2 Verringerung der Lohnnebenkosten. (Quelle: eigene Darstellung)

Durchführungsweg	Arbeitgeberfinanzierung	Arbeitnehmerfinanzierung (Entgeltumwandlung)
Direktversicherung	beitragsfrei bis 4 % der BBG	beitragsfrei bis 4 % der BBG
Pensionsfonds	beitragsfrei bis 4 % der BBG	beitragsfrei bis 4 % der BBG
Pensionskasse	beitragsfrei bis 4 % der BBG	beitragsfrei bis 4 % der BBG
Unterstützungskasse	beitragsfrei*	beitragsfrei bis 4 % der BBG
Direktzusage	beitragsfrei*	beitragsfrei bis 4 % der BBG

*kann additiv zu den Durchführungswegen Direktversicherung, Pensionsfonds, und Pensionskasse genutzt werden

Da die steuerliche Wirkung sehr komplex und sowohl vom gewählten Durchführungs-
weg als auch von der konkreten Ausgestaltung abhängig ist, hier nur stark verkürzte allge-
meine Aussagen.

Direktversicherung: Beiträge hierfür sind voll als Betriebsausgabe abzugsfähig und
mindern den zu versteuernden Gewinn.

Pensionskasse: Beiträge hierfür sind voll als Betriebsausgabe abzugsfähig und
mindern den zu versteuernden Gewinn.

Pensionsfonds: Der Arbeitgeber darf Beiträge an einem Pensionsfonds leisten,
wenn hiermit festgelegte Versorgungsleistungen finanziert oder
Fehlbeträge des Pensionsfonds ausgeglichen werden. Diese Bei-
träge sind dann als Betriebsausgaben abzugsfähig. § 4 e EStG.

Unterstützungskasse: Beiträge hierfür sind grundsätzlich als Betriebsausgabe abzugs-
fähig und mindern den zu versteuernden Gewinn.

Direktzusage: Rückstellungsbildung, Passivierung ist ein Aufwand/Betriebs-
ausgabe und somit steuermindernd. Das Unternehmen hat hier-
mit einen Liquiditätsgewinn/eine Form der Innenfinanzierung.

Bei einer rückgedeckten Direktzusage sind die Beiträge in voller Höhe Betriebsaus-
gabe. Allerdings gehört der angesparte Wert der Versicherung zum Betriebsvermögen und
muss aktiviert werden = Gewinn- und somit steuererhöhend (vgl. Buttler und Keller 2017,
S. 142).

Bei der Einrichtung einer bAV sollte daher unbedingt neben einem Versicherungsver-
mittler auch ein auf bAV-Lösungen spezialisierter Steuerberater hinzugezogen werden.

31.2.2 Personengruppen und Rechtsanspruch

Arbeitnehmer haben einen gesetzlichen Anspruch auf Entgeltumwandlung aus § 1a BetrAVG. Der Arbeitnehmer kann somit von seinem Arbeitgeber die Umwandlung von Gehalts-
bestandteilen in eine Direktversicherung verlangen, sofern der Arbeitgeber die betriebliche
Altersversorgung nicht über eine vorgegebene Versorgungseinrichtung, einen Pensionsfonds
oder eine Pensionskasse anbietet. Die im § 1a BetrAVG vereinfacht zusammengefassten
Arbeitnehmer bestehen aus verschiedenen Personengruppen. Diese werden in § 17 Abs. 1
BetrAVG aufgeführt und umfassen Auszubildende, Arbeiter und Angestellte.

31.2.3 Arbeitsrechtliche Grundlagen

Entschließt sich ein Arbeitgeber zur Einrichtung einer betrieblichen Altersversorgung,
dann ist er an die Regelungen des Betriebsrentengesetzes (BetrAVG) gebunden. Insofern
bildet das BetrAVG den gesetzlichen Rahmen. Jegliche bAV beruht auf einer arbeitsrecht-
lichen Zusage des Arbeitgebers – ganz gleich, welcher Durchführungsweg gewählt wird.

Das BetrAVG gibt als Arbeitnehmerschutzgesetz Mindestnormen vor. Abweichungen zum Nachteil der Arbeitnehmer sind grundsätzlich nicht zulässig, außer, ein Tarifvertrag sieht dies vor. Neben dem BetrAVG bilden individuelle und kollektive vertragliche Vereinbarungen die Basis der betrieblichen Altersversorgung.

31.2.3.1 Zusage

Nach § 1 Abs. 1 BetrAVG liegt eine bAV vor, wenn ein Arbeitgeber seinem Arbeitnehmer Leistungen auf Alters-, Invaliditäts- oder Hinterbliebenenversorgung aus Anlass eines Arbeitsverhältnisses zusagt. Hinterbliebene sind dabei Ehe- oder Lebenspartner (auch frühere Ehepartner) und Kinder. Es wird zwischen verschiedenen Zusageformen unterschieden:

- **Leistungszusage:** Hier sagt der Arbeitgeber dem Arbeitnehmer eine klar definierte Leistung zu, zum Beispiel einen festen Eurobetrag oder einen bestimmten Prozentsatz des letzten Gehaltes (§ 1 Abs. 1 BetrAVG).
- **Beitragsorientierte Leistungszusage:** Hier verpflichtet sich der Arbeitgeber, für eine bestimmte Leistung seiner Arbeitnehmer entsprechende Beiträge in eine Anwartschaft auf Alters-, Invaliditäts- oder Hinterbliebenenversorgung aufzuwenden (§ 1 Abs. 2 Nr. 1 BetrAVG).
- **Beitragszusage mit Mindestleistung:** Hier verpflichtet sich der Arbeitgeber lediglich, bestimmte Beiträge an einen Pensionsfonds, eine Pensionskasse oder eine Direktversicherung zu zahlen, aus denen der Arbeitnehmer die sich daraus ergebene Versorgungsleistung erhält. Als Mindestleistung sagt der Arbeitgeber den Beitragserhalt zzgl. ggf. erzielter Erträge zu (§ 1 Abs. 2 Nr. 2 BetrAVG).
- **Reine Beitragszusage:** Dies ist eine ausschließliche Verpflichtung, die vereinbarten Beiträge an den Versorgungsträger zu leisten. Es entsteht keinerlei Nachhaftung für den Arbeitgeber (§ 1 Abs. 2 Nr. 2a BetrAVG).

31.2.3.2 Weitere Anspruchsgrundlagen

Wie bereits dargelegt, bildet das BetrAVG die rechtliche Basis. Darüber hinaus gibt es noch weitere Grundlagen. Die Zusagen können einzelvertraglich oder an bestimmte Gruppen im Betrieb kollektiv-vertraglich aufgrund einer Betriebsvereinbarung oder Tarifvertrags erklärt werden.

Einzelvertragliche Zusage

Diese Zusage entsteht, wenn der Arbeitgeber gegenüber seinen Mitarbeitern eine entsprechende Erklärung abgibt. Eine Schriftform ist nicht erforderlich. Es genügt zum Beispiel, wenn die Einrichtung der bAV im Rahmen einer Betriebsversammlung verkündet wird. Die Regelung wird dann Bestandteil jedes einzelnen Arbeitsvertrages.

Betriebsvereinbarung

Üblicherweise (gerade bei größeren Unternehmen) wird bei Einrichtung einer bAV eine Betriebsvereinbarung geschlossen. Diese Vereinbarung wird zwar nicht Bestandteil eines jeden einzelnen Arbeitsvertrages, ihre Regelungen sind aber dennoch für alle Arbeitnehmer verbindlich.

Hierdurch können später notwendige Änderungen am Versorgungswerk leichter umgesetzt werden.

Tarifvertrag

Ansprüche auf Gewährung einer bAV können sich auch aus einem Tarifvertrag ergeben. Üblicherweise werden hier jedoch nur Rahmenbedingungen bzw. Mindeststandards festgelegt, so zum Beispiel das Volumen der Zusage oder der Durchführungsweg. Es empfiehlt sich, die notwendigen Details in einer Versorgungsordnung zu regeln. Diese Versorgungsordnung kann dann auch wiederum zum Beispiel im Rahmen einer Betriebsvereinbarung arbeitsrechtlich geregelt werden.

Betriebliche Übung

Eine Zusage auf bAV kann durchaus auch aus einer betrieblichen Übung entstehen. Eine betriebliche Übung kann vorliegen, wenn der Arbeitgeber durch wiederholtes Verhalten erkennen lässt, dass er beim Vorliegen bestimmter Voraussetzungen Versorgungsleistungen zusagt oder erbringt. Durch eine betriebliche Übung werden freiwillige Leistungen des Arbeitgebers zu verpflichtenden, denen sich der Arbeitgeber dann nicht mehr einseitig entziehen kann. Gewährt zum Beispiel ein Arbeitgeber über Jahre hinweg allen Mitarbeitern eine Altersrente, sobald sie in den Ruhestand eintreten, so erlangen ggf. auch die noch aktiven Beschäftigten einen Anspruch auf Gewährung einer solchen Rente (vgl. Buttler und Keller 2017, S. 32).

31.2.3.3 Mitbestimmung

Grundsätzlich entscheidet der Arbeitgeber frei, ob und in welcher Form und für welche Arbeitnehmer er eine bAV einführt. In mitbestimmten Unternehmen unterliegen aber einige Details der Mitbestimmung durch den Betriebsrat. Das BetrAVG enthält hierzu keine Vorschriften, allerdings gelten die Vorschriften des Betriebsverfassungsgesetzes (BetrVG).

Nach § 87 Abs. 1 Nr. 8 und 10 BetrVG hat der Betriebsrat über die Form, Ausgestaltung und Verwaltung von Sozialeinrichtungen und zu Fragen der betrieblichen Lohngestaltung und deren Grundsätzen mitzubestimmen.

31.2.3.4 Haftung des Arbeitgebers

Zunächst haftet der Arbeitgeber für die Erfüllung seiner unmittelbaren Zusagen im Rahmen einer Direktzusage oder Unterstützungskasse. Darüber hinaus haftet der Arbeitgeber aber auch für die Leistungserbringung einer unmittelbaren Zusage im Rahmen eines Pensionsfonds, einer Pensionskasse oder einer Direktversicherung nach § 1 Abs. 1 S. 3 BetrAVG.

Der Umfang der Haftung bestimmt sich nach der Zusageart: Bei Leistungszusagen und beitragsorientierten Leistungszusagen trägt der Arbeitgeber das Anlage- und Renditerisiko. Denn die Zahlungsverpflichtung gemäß der Zusage muss ja erfüllt werden, auch wenn die einkalkulierte Rendite nicht erwirtschaftet wird. Bei der Beitragszusage mit Mindestleistungen ist die Haftung des Arbeitgebers reduziert, da er lediglich für den Erhalt der eingezahlten Beiträge einstehen muss.

Keine Haftung trifft den Arbeitgeber, wenn aufgrund tarifvertraglicher Vereinbarung lediglich eine reine Beitragszusage erteilt wurde. Der Arbeitgeber hat dann nur die Pflicht, die Beiträge abzuführen.

31.2.3.5 Anspruch auf Entgeltumwandlung

Alle Arbeitnehmer, die in der gesetzlichen Rentenversicherung pflichtversichert sind, haben nach § 1a in Verbindung mit § 17 BetrAVG einen Rechtsanspruch auf Umwandlung von Gehaltsteilen in eine betriebliche Altersversorgung.

Das Recht auf Entgeltumwandlung besteht bis zu einer Höhe von vier Prozent der jeweiligen Betragsbemessungsgrenze (West) der Rentenversicherung. In 2020 sind dies bis zu 3312 Euro jährlich.

31.2.3.6 Arbeitgeberzuschuss

Nutzt ein Arbeitnehmer sein Recht auf Entgeltumwandlung, ist der Arbeitgeber verpflichtet, einen Zuschuss in Höhe von 15 Prozent des umgewandelten Betrages zu zahlen (§ 1a Abs. 1a BetrAVG).

Dies gilt nur, soweit der Arbeitgeber eine Sozialversicherungsersparnis hat. Spart er keine Sozialversicherungsbeiträge ein, weil der Arbeitnehmer zum Beispiel ein Einkommen oberhalb der Beitragsbemessungsgrenze bezieht, muss er auch keinen Zuschuss leisten.

Erzielt ein Arbeitnehmer ein Einkommen oberhalb der Beitragsbemessungsgrenze der Krankenversicherung, aber unterhalb der Beitragsbemessungsgrenze der Rentenversicherung, so kann es sein, dass der Arbeitgeber zwar eine Sozialversicherungsersparnis hat, diese aber kleiner als 15 Prozent des Umwandlungsbetrages ist. Da die individuelle Sozialversicherungsersparnis eines jeden Arbeitnehmers ausschlaggebend ist, muss nicht pauschal 15 Prozent abgeführt werden, sondern nur die tatsächlich erzielte Ersparnis (vgl. Meissner et al. 2018, S. 75 ff.).

Diese Regelung ist sehr aufwendig und führt im Grunde dazu, jedes Jahr für jeden Arbeitnehmer die Ersparnis neu zu berechnen. Viele Unternehmen gehen daher den Weg, pauschal 15 Prozent zu bezuschussen, wenn überhaupt eine Sozialversicherungsersparnis vorliegt- unabhängig von der tatsächlichen Höhe.

31.2.3.7 Unverfallbarkeit

Scheidet ein Arbeitnehmer vorzeitig aus dem Unternehmen aus, so kann er durchaus einen Anspruch auf Teile der zugesagten Leistungen erwirkt haben. Hier spricht man von einem „unverfallbaren Anspruch“ des Arbeitnehmers. Entscheidend ist das Zusagedatum.

Handelt es sich um eine rein arbeitnehmerfinanzierte Versorgung (Bruttoentgeltumwandlung), hat der (ehemalige) Mitarbeiter sofort einen unverfallbaren Anspruch, ganz gleich, wie lange die Beschäftigung dauerte (§ 1b Abs. 5 BetrAVG).

Handelt es sich um eine arbeitgeberfinanzierte Zusage, ist die Unverfallbarkeit – neben der Dauer der Beschäftigung – vom erreichten Lebensalter abhängig.

Tab. 31.3 beschreibt die Voraussetzungen.

31.2.3.8 Portabilität bei Wechsel des Arbeitgebers

Wechselt ein Arbeitnehmer seinen Arbeitgeber, sind bis dahin erworbene Versorgungsansprüche grundsätzlich übertragbar. Dies bezeichnet man als „Portabilität“. Sowohl der bisherige als auch der neue Arbeitgeber und auch der Arbeitnehmer müssen hiermit einverstanden sein (§ 4 Abs. 2 BetrAVG).

Die beim bisherigen Arbeitgeber erworbenen Anwartschaften können in einem bestimmten Wert umgerechnet werden. Dieser sogenannte „Übertragungswert“ kann dann in das Versorgungssystem des neuen Arbeitgebers eingebracht werden und dieser erteilt dann auf Basis des mitgebrachten Kapitals eine „wertgleiche Zusage“.

Es besteht auch die Möglichkeit, dass der neue Arbeitgeber die bisherige Zusage identisch übernimmt. Der neue Arbeitgeber tritt dann mit allen Rechten und Pflichten in die Rechtsstellung des früheren Arbeitgebers ein. Für Zusagen ab dem 01.01.2005 besteht nach § 4 Abs. 3 Nr. 1 und 2 BetrAVG sogar ein Rechtsanspruch des Arbeitnehmers gegen seinen bisherigen Arbeitgeber auf Übertragung des Werts der unverfallbaren Ansprüche auf den neuen Arbeitgeber. Voraussetzung hierfür ist allerdings, dass die betriebliche Altersversorgung über die Durchführungswege Pensionsfonds, Pensionskasse oder Direkt-

Tab. 31.3 Unverfallbarkeitsvoraussetzungen. (Quelle: Wissenschaftliche Dienste; Deutscher Bundestag (o. V. 2019, S. 15))

	Arbeitgeber-finanzierte Zusagen ab 2018	Arbeitgeber-finanzierte Zusagen von 2009 bis 2017	Arbeitgeber-finanzierte Zusagen von 2001 bis 2008	Arbeitgeberfinanzierte Zusagen bis 2000
Unverfallbarkeitsfrist	Zusage mindestens drei Jahre vor Ende der Beschäftigung	Zusage mindestens fünf Jahre vor Ende der Beschäftigung	Zusage mindestens fünf Jahre vor Ende der Beschäftigung	Zusage mindestens zehn Jahre vor Ende der Beschäftigung oder Zusage mind. drei Jahre vor Ende der Beschäftigung bei mind. zwölfjähriger Betriebszugehörigkeit
Lebensalter des AN bei Ende der Beschäftigung	21	25	30	35
Grundlage	§ 1b Abs. 1 BetrAVG	§ 30 f Abs. 3 BetrAVG	§ 30 f Abs. 2 BetrAVG	§ 30 f Abs. 1 BetrAVG

versicherung erfolgte und der Übertragungswert die Beitragsbemessungsgrenze in der allgemeinen Rentenversicherung West (2020: 82.800 Euro) nicht übersteigt.

Steuerlich betrachtet handelt es sich bei der Übertragung um eine Art „Abfindung“ des alten Arbeitgebers und um eine Wiedereinzahlung bei dem neuen Arbeitgeber (vgl. Buttler und Keller 2017, S. 74). Unter bestimmten Voraussetzungen sind diese Übertragungen steuerfrei. So zum Beispiel, wenn die Übertragung innerhalb der internen Durchführungswege (Direktzusage und Unterstützungskasse) oder der externen Durchführungswege (Pensionsfonds, Pensionskasse und Direktversicherung) erfolgt. Näheres regelt § 3 Nr. 55 EStG.

31.2.3.9 Beginn der Leistung

Grundsätzlich richtet sich der Leistungsbeginn nach dem Inhalt der erteilten Zusage. Auf Verlangen des Arbeitnehmers beginnen die Altersrentenleistungen nach § 6 BetrAVG aber spätestens mit der Zahlung der Vollrente der gesetzlichen Rentenversicherung.

Fällt die Altersrente aus der gesetzlichen Rentenversicherung wieder weg oder wird sie auf einen Teilbetrag beschränkt, so können auch die Leistungen der betrieblichen Altersversorgung eingestellt werden (§ 6 S. 2 BetrAVG).

31.2.3.10 Anpassung der Leistungen

Der Arbeitgeber hat nach § 16 BetrAVG die Pflicht, alle drei Jahre eine Anpassung der laufenden Betriebsrenten zu prüfen und ggf. durchzuführen. Dabei ist auch die wirtschaftliche Lage des Unternehmens zu berücksichtigen. Die Verpflichtung gilt als erfüllt, wenn die Anpassung nicht geringer ist als der Anstieg des Verbraucherpreisindexes für Deutschland oder der Nettolöhne vergleichbarer Arbeitnehmergruppen des Unternehmens.

Diese Verpflichtung gilt nicht, wenn der Arbeitgeber sich verpflichtet, die laufenden Leistungen jährlich um ein Prozent anzupassen (§ 16 Abs. 3 Nr. 1 BetrAVG).

Ferner besteht die Verpflichtung nicht, wenn die betriebliche Altersversorgung über eine Direktversicherung oder über eine Pensionskasse durchgeführt wird und ab Rentenbeginn sämtliche auf den Rentenbestand entfallende Überschussanteile zur Erhöhung der laufenden Leistungen verwendet werden (§ 16 Abs. 3 Nr. 2 BetrAVG).

Auch bei Beitragszusagen mit Mindestleistung entfällt die Anpassungspflicht nach § 16 Abs. 3 Nr. 3 BetrAVG.

Bei der reinen Entgeltumwandlung ist der Arbeitgeber verpflichtet, die Leistungen mindestens um ein Prozent p.a. anzupassen oder im Falle der Durchführung über eine Direktversicherung oder eine Pensionskasse sämtliche Überschussanteile zur Leistungserhöhung zu verwenden (§ 16 Abs. 5 BetrAVG).

31.2.4 Steuerliche und sozialversicherungsrechtliche Behandlung

Die steuerliche Behandlung der Beiträge und Leistungen der bAV hängt von dem gewählten Durchführungsweg und den jeweiligen Regelungen des Einkommenssteuergesetzes ab. Um einen möglichst kompakten und gleichzeitig umfassenden Überblick über die je-

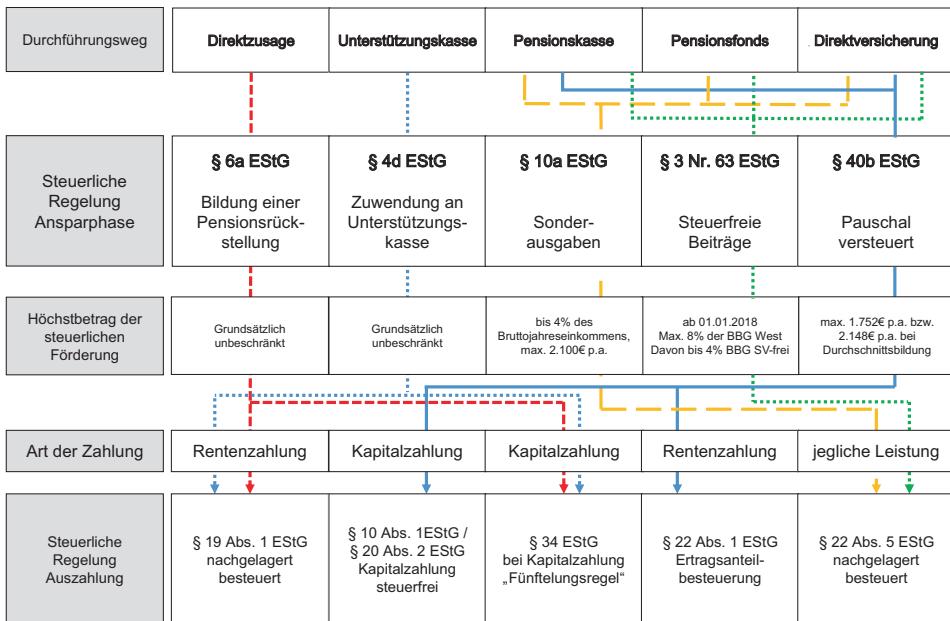


Abb. 31.2 Steuerliche Behandlung der Durchführungswege. (Quelle: eigene Darstellung)

weiligen Regelungen zu verschaffen, zeigt Abb. 31.2 die steuerliche Behandlung der Durchführungswege. Hierbei wird bei den Durchführungswegen Pensionskasse, Pensionsfonds und Direktversicherung die Arbeitnehmersicht eingenommen. Die „Steuerliche Regelung Auszahlung“ wird ebenfalls aus Sicht des Arbeitnehmers dargestellt. Je nach Durchführungswege stehen mehrere Möglichkeiten zur Auswahl, die durch die Grafik von oben nach unten entlang der Pfeile abgelesen werden können. Bei manchen der Durchführungswege können verschiedene Regelungen des EStG Anwendung finden. So kann die Direktversicherung beispielsweise nach § 10a EStG (Riesterförderung) als Sonderausgabe steuerlich geltend gemacht werden, aber auch über § 3 Nr. 3 EStG (bAV, Zusage ab 2005) und nach § 40b EStG pauschal versteuert sein (bAV, Zusage bis 2005). Zur Auszahlung muss noch angemerkt werden, dass die Leistungen aus bAV der Sozialversicherungspflicht unterliegen. Konkret bedeutet dies, dass gesetzlich Krankenversicherte Beiträge zur Kranken- und Pflegeversicherung zahlen müssen. Im Jahr 2020 sind dies 14,6 Prozent zuzüglich des kassenindividuellen Zusatzbeitrages. Bei einer einmaligen Kapitalauszahlung, anstatt Rentenzahlung, wird auf den Auszahlungsbetrag dieser Krankenversicherungsbeitrag berechnet und auf 120 Monatsraten (auch „120tel-Regelung“ genannt) verteilt, sodass folglich zehn Jahre lang ein monatlich gleichbleibender Betrag gezahlt werden muss. Mithin ergibt sich durch Steuern und Sozialabgaben eine Minderung der Leistungen. Zudem kann eine Minderung des rentenversicherungspflichtigen Einkommens durch Entgeltumwandlung zu einer verringerten gesetzlichen Rente führen.

Auf die Unterschiede der jeweiligen Durchführungswege (vgl. Abb. 31.2) wird später vertieft eingegangen.

31.2.5 Zusagearten und Finanzierung

Die Zusagearten der bAV lassen sich zunächst in unmittelbare und mittelbare Zusagen einteilen. Bei der Direktzusage wird eine Leistung an den Arbeitnehmer unmittelbar und somit ohne weitere zwischengeschaltete Träger zugesagt. Mithin entsteht ein Rechtsverhältnis zusätzlich zum Arbeitsvertrag. Im Gegensatz hierzu stehen die mittelbaren Zusagen in den Durchführungswege Direktversicherung, Pensionsfonds, Pensionskasse und Unterstützungskasse. Bei diesen Zusagen wird eine externe Versorgungseinrichtung oder eine Versicherung zwischengeschaltet und diese übernimmt die Verwaltung und Anlage des Geldes sowie die Erbringung der zugesagten Leistungen. Die Zusage an sich kann in Form einer Leistungszusage, einer beitragsorientierten Leistungszusage (BOLZ), einer beitragsorientierten Leistungszusage mit Mindestleistung (BZML) oder der, im Zuge des Betriebsrentenstärkungsgesetzes neu eingeführten, reinen Beitragszusage bestehen (vgl. Abschn. 31.2.3.1). Nur die reine Beitragszusage weist keine Subsidiärhaftung des Arbeitgebers auf. Jedoch ist die reine Beitragszusage nur im so genannten Sozialpartnermodell möglich.

Die Finanzierung der bAV kann grundsätzlich entweder vollständig durch den Arbeitgeber (arbeitgeberfinanziert), vollständig durch den Arbeitnehmer im Rahmen der Entgeltumwandlung ohne Arbeitgeberzuschuss (arbeitnehmerfinanziert), oder im Rahmen einer Entgeltumwandlung mit Beteiligung des Arbeitgebers in Form eines Zuschusses (mischfinanziert) durchgeführt werden. Welche Finanzierungsform gewählt wird, hängt von tarifvertraglichen Regelungen und den Vereinbarungen im Betrieb ab. Seit dem 01.01.2019 besteht für Neuzusagen jedoch durch das Betriebsrentenstärkungsgesetz grundsätzlich eine Verpflichtung zur Bezuschussung von Entgeltumwandlungsbeträgen mit einem Betrag in Höhe von 15 Prozent der umgewandelten Entgeltbestandteile, soweit der Arbeitgeber Sozialabgaben spart. Für bestehende (Alt-)Zusagen vor dem 01.01.2019 greift die Zuschusspflicht erst ab dem 01.01.2022. Mithin sollten die rein arbeitnehmerfinanzierten Betriebsrenten zukünftig eher eine untergeordnete Rolle spielen.

31.2.6 Durchführungswege

In diesem Abschnitt werden die fünf Durchführungswege der betrieblichen Altersversorgung in einem Kurzüberblick beschrieben und es wird auf die Bilanzberührung eingegangen. Es bestehen insgesamt die nachfolgenden fünf Durchführungswege: Direktversicherung, Pensionsfonds, Pensionskasse und die Direktzusage.

Direktversicherung

Bei diesem Durchführungsweg handelt es sich um eine vom Arbeitgeber auf das Leben des Arbeitnehmers abgeschlossene Lebensversicherung, meist in Form einer Rentenversicherung. Der versicherte Arbeitnehmer hat hierbei einen Rechtsanspruch auf Leistung gegenüber dem Lebensversicherer. Der Arbeitgeber ist der Versicherungsnehmer des Vertrags.

ges, der Arbeitnehmer ist der Bezugsberechtigte. Bei Einschluss einer Todesfallleistung können auch Hinterbliebene bezugsberechtigt sein. Die Direktversicherung zeichnet sich dadurch aus, dass sich die Einrichtung eines solchen Vertrages vergleichsweise einfach gestaltet und es beim Arbeitgeber zu keiner Bilanzberührung kommt. Sie ist im Jahresabschluss ergebnisneutral.

Pensionsfonds

Ein Pensionsfonds ist eine rechtsfähige Versorgungseinrichtung zum Zweck der betrieblichen Altersversorgung in Form einer Aktiengesellschaft oder eines Versicherungsvereins auf Gegenseitigkeit. Der Arbeitnehmer hat einen Rechtsanspruch gegen den Pensionsfonds. Finanziert werden die Leistungen des Pensionsfonds durch Beiträge des Arbeitgebers, die für den Arbeitnehmer eingezahlt werden. Diese Beiträge können nach § 4e EStG als Betriebsausgaben abgesetzt werden. Jedoch sind die Beiträge nicht allein vom Arbeitgeber zu entrichten, es können auch Entgeltbestandteile des Arbeitnehmers in Form einer arbeitnehmer- oder mischfinanzierten Entgeltumwandlung eingezahlt werden. Grundsätzlich haben Pensionsfonds in ihrer Kapitalanlage mehr Freiheitsgrade als die Direktversicherung oder Pensionskasse. Pensionsfonds werden jedoch durch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) überwacht und sind somit mit Pensionskassen und Lebensversicherern vergleichbar. In der Unternehmensbilanz ist der Pensionsfonds grundsätzlich bilanzneutral.

Pensionskasse

Pensionskassen sind ebenfalls rechtsfähige Versorgungseinrichtungen zum Zweck der betrieblichen Altersversorgung, die eine spezielle Art von Lebensversicherern darstellen. Wie beim Pensionsfonds zahlt der Arbeitgeber die Beiträge an die Versorgungseinrichtung und der Arbeitnehmer kann sich durch Entgeltumwandlung an diesen Beiträgen beteiligen. Wie beim Pensionsfonds hat der Arbeitnehmer einen Rechtsanspruch gegen die Pensionskasse. Es gilt allerdings zwischen regulierten und deregulierten Pensionskassen zu unterscheiden. Grundsätzlich sind Pensionskassen dereguliert, können aber unter bestimmten Voraussetzungen auf Antrag der Kasse von der BaFin reguliert werden. Die Kapitalanlagemöglichkeiten sind bei Pensionskassen deutlich eingeschränkter und ähneln denen klassischer Lebensversicherungsanlagen.

Unterstützungskasse

Auch bei der Unterstützungskasse handelt es sich um eine rechtsfähige Versorgungseinrichtung zum Zweck der betrieblichen Altersversorgung. Jedoch hat der Arbeitnehmer keinen direkten Rechtsanspruch gegen die Versorgungseinrichtung. Finanziert wird diese Versorgungseinrichtung, die in Form eines Vereins, einer Stiftung oder einer GmbH geführt werden kann, durch Beiträge/Dotierungen eines oder mehrerer Trägerunternehmen. Die Unterstützungskasse unterliegt nicht der Aufsicht durch die BaFin und hat somit erhebliche Freiheitsgrade bei der Kapitalanlage. Unterschieden werden muss hierbei allerdings zwischen der rückgedeckten Unterstützungskasse und der pauschaldotierten Unterstützungs-

kasse. Bei der rückgedeckten Unterstützungskasse wird eine Rückdeckungsversicherung analog einer Rentenversicherung abgeschlossen, mit der die Leistungen ausfinanziert werden. Die pauschaldotierte Unterstützungskasse hingegen kann die Kapitalanlage frei wählen und das Kapital sogar in Form von Darlehen an das Trägerunternehmen anlegen. Durch diese Form der „Anlage“ kann das Trägerunternehmen Liquidität gewinnen.

Direktzusage

Dieser Durchführungsweg unterscheidet sich in mehreren Punkten von den zuvor aufgeführten Durchführungswegen. Die Direktzusage, oder auch Pensionszusage genannt, stellt eine Verpflichtung des Arbeitgebers gegenüber dem Arbeitnehmer dar. Meist werden die Beiträge vollständig vom Arbeitgeber finanziert und im Eintritt des Versorgungsfalles ist der Arbeitgeber direkt dem Arbeitnehmer gegenüber zur Zahlung verpflichtet. Insbesondere bei vorzeitigen Versorgungsfällen wie Invaliditäts- oder Todesfallleistungen kann es dazu kommen, dass diese Leistungen eine nicht einkalkulierte Belastung darstellen. Die Höhe der Altersrente richtet sich nicht nach einem Beitrag, sondern wird als Festbetrag (absolute Höhe des Rentenbetrags) oder durch einen Endgehältsplan (prozentuale Rente berechnet anhand der Höhe des letzten Gehalts) festgelegt.

Ein weiterer Unterschied ist die Bilanzierung der Zahlungsverpflichtungen in Form von Pensionsrückstellungen gemäß § 249 HGB in Verbindung mit § 6a EStG. Diese Rückstellungen in Form eines Barwertes müssen nach versicherungsmathematischen Grundsätzen ermittelt werden und sind in der Bilanz gewinnmindernd. Bei einer Auflösung der Rückstellung ist der frei werdende Betrag gewinnerhöhend zu verbuchen. In der Rentenphase stellen die Zahlungen an den Arbeitnehmer einen Aufwand dar. Um die Zahlungsverpflichtungen zu Rentenbeginn auch wirklich bedienen zu können reicht es nicht aus, nur eine Rückstellung zu bilden, denn dies ist nur bilanziell geschehen. Das Kapital muss auch zu Rentenbeginn des Arbeitnehmers tatsächlich zur Verfügung stehen. Hierzu kann eine kongruente oder anteilige Rückdeckungsversicherung abgeschlossen werden. Direktzusagen werden primär von großen Unternehmen und für hohe Zusagen eingerichtet, da der mit der Bildung und Finanzierung verbundene Aufwand nicht von der Hand zu weisen ist.

31.2.7 Betriebsrentenstärkungsgesetz

Das Betriebsrentenstärkungsgesetz (BRSG) wurde im August 2017 beschlossen und stellt eine bedeutende Reform für die ergänzende Altersversorgung dar. Auf die wesentlichen Punkte dieses Gesetzes wird im Folgenden eingegangen. Ziel des Gesetzes ist es, die Verbreitung betrieblicher Altersversorgung zu fördern (Bundesfinanzministerium 2017). Dies gilt insbesondere für kleine und mittlere Unternehmen (vgl. hierzu auch Abschn. 31.1.). Die Änderungen treten zeitversetzt in drei Stufen jeweils zum Jahresanfang des Jahres 2018, 2019 und 2022 in Kraft.

Zum 01.01.2018 wurden zahlreiche Änderungen umgesetzt. Diese betreffen allerdings nicht nur die bAV, sondern teilweise auch die private Altersvorsorge. Im Zuge des BRSG wurde beispielsweise die Zulage für Riesterrenten-Verträge von 154 Euro auf 175 Euro erhöht. Zudem unterliegen fortan Leistungen der Riesterrente, sowohl privat als auch neu über den Arbeitgeber, nicht mehr der Sozialversicherungspflicht. Somit wurde die so genannte „Riester-bAV“ der privaten Riesterrente gleichgestellt. Neben diesen Veränderungen wurden zudem die Riesterrente und die bAV weiter gestärkt, indem ein Freibetrag zur Anrechnung auf die Grundsicherung und die Erwerbsminderungsrente eingeführt wurde. Bislang wurde im Falle einer geringen Rente im Rahmen der Grundsicherung aufgestockt, was dazu führte, dass Riester- und Betriebsrenten auf den Aufstockungsbetrag angerechnet wurden, und so lediglich der Aufstockungsbetrag reduziert wurde. Diese oftmals als Ungerechtigkeit empfundene Anrechnung ist seit dem 01.01.2018 für bestehende Leistungsempfänger und alle zukünftigen Leistungsbezieher beseitigt. Der Sockelfreibetrag ist mit 100 Euro angesetzt und wird durch einen prozentualen erweiterten Freibetrag in Höhe von 30 Prozent ergänzt. Dieser gesamte Freibetrag ist auf die Hälfte der Regelbedarfsstufe 1 (geregelt in Anlage zu § 28 SGB zwölftes Buch) festgesetzt. Im Jahr 2020 beträgt die benannte Regelbedarfsstufe 432 Euro. Somit liegt für das Jahr 2020 der maximale Freibetrag bei 216 Euro monatlich.

Ebenfalls zum 01.01.2018 wurde neben die bereits existierende „bAV-Welt I“ eine neue „bAV-Welt II“ gesetzt. Diese besteht aus dem sogenannten Sozialpartnermodell, welches in der Praxis teilweise auch als „Sechster Durchführungsweg“ betitelt wird. Die Grundidee des Sozialpartnermodells ist es, dass Tarifvertragsparteien sich auf eine betriebliche Altersversorgung einigen und „sich an deren Durchführung und Steuerung beteiligen“ (§ 21 BetrAVG). Abb. 31.3 verdeutlicht das Konzept des Sozialpartnermodells und die Beziehungen zwischen den beteiligten Parteien. Diese betriebliche Altersversorgung muss in den Durchführungs wegen Direktversicherung, Pensionskasse oder Pensionsfonds erfolgen und besteht aus einer reinen Betragszusage und umfasst ein Verbot von Garantien (§ 244b VAG).

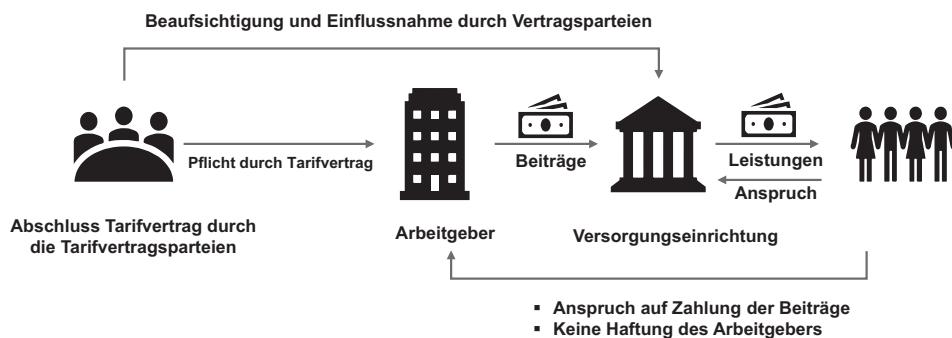


Abb. 31.3 Beziehungen der am Sozialpartnermodell beteiligten Parteien. (Quelle: eigene Darstellung)

31.3 Beachtenswerte Punkte aus der Praxis

31.3.1 Gleichbehandlung

Ein wichtiger Grundsatz bei der bAV stellt der Aspekt der Gleichbehandlung dar. Dieser wird in § 1b Abs. 1 S. 4 BetrAVG wörtlich genannt. So dürfen ohne Vorliegen sachlicher Gründe einzelne Arbeitnehmer oder Arbeitnehmergruppen nicht benachteiligt werden. Ein Beispiel von Ungleichbehandlung ist die unterschiedliche Höhe des Arbeitgeberzuschusses innerhalb einer gleichartigen Personengruppe. In der Praxis könnte ein Arbeitgeber auf die Idee kommen, der Mehrheit von Mitarbeitern einer gleichartigen Personengruppe anstatt einer Gehaltserhöhung eine arbeitgeberfinanzierte betriebliche Altersversorgung anzubieten, während er bestimmten Mitarbeitern nur einen geringen Zuschuss zahlt. Explizit ausgeschlossen ist die Bevorzugung eines Arbeitnehmers nicht, es darf jedoch nicht zu einer Benachteiligung anderer Arbeitnehmer führen. Die in diesem Sinne benachteiligten Mitarbeiter könnten dann ggf. versuchen, einen Anspruch gegenüber dem Arbeitgeber geltend zu machen. Aus diesen angeführten Gründen ist eine Gleichbehandlung der Mitarbeiter und Mitarbeitergruppen zu empfehlen. Bei der Bevorzugung von Mitarbeitern sollten alle sachlichen Gründe für die Bevorzugung minutiös dokumentiert werden.

Ebenfalls eine gelegentlich auftauchende Ungleichbehandlung ist bei mitarbeitenden Ehepartnern und Familienangehörigen des Firmeninhabers zu beobachten. Diese dürfen nicht ohne sachlich und rechtlich einwandfreie Gründe eine höhere betriebliche Zusage erhalten, als sie andere familienfremde Mitarbeiter bekommen würden. Die Zusage an Familienangehörige muss angemessen sein. Andernfalls könnte unter bestimmten Voraussetzungen die steuerliche Anerkennung verwehrt werden (zum Beispiel im Rahmen eines Fremdvergleiches oder bei Vorliegen einer Überversorgung).

31.3.2 Entgeltumwandlungsvereinbarung und Versorgungsordnung

Bei der Entgeltumwandlungsvereinbarung handelt es sich um eine Vereinbarung zwischen Arbeitgeber und Arbeitnehmer zur Umwandlung von Entgeltbestandteilen in eine bAV. Sie versteht sich als eine Abänderung des Dienstvertrages, denn in diesem wird ja festgehalten, wie hoch das Entgelt des Arbeitnehmers ist. In der Entgeltumwandlungsvereinbarung sind auch etwaige Arbeitgeberzuschüsse zur bAV geregelt, sofern es sich um eine mischfinanzierte bAV handelt. Diese Vereinbarung sollte gründlich formuliert sein und von Arbeitgeber und Arbeitnehmer unterzeichnet werden, um Klarheit zu schaffen und rechtliche Auseinandersetzungen vorzubeugen. Im Zuge des Betriebsrentenstärkungsgesetzes wurde, wie bereits in Abschn. 31.2.3.6 erläutert, ein verbindlicher Arbeitgeberzuschuss beschlossen, der für neue Zusagen seit dem 01.01.2019 greift, für bestehende Zusagen ab 01.01.2022. In diesem Zusammenhang sollte aus Arbeitgebersicht ein Passus enthalten sein, der die Anrechnung auf spätere gesetzlich verpflichtende Zuschüsse, insbesondere

auch aus Sozialabgabenersparnis, eindeutig impliziert. Ein Fehlen dieser Formulierung könnte sonst möglicherweise dazu führen, dass der Arbeitgeber zwar bereits einen Zuschuss zahlt, dieser aber nicht auf die verpflichtenden 15 Prozent Zuschuss ab dem 01.01.2022 angerechnet wird. So könnte es unter Umständen zu einer zusätzlichen Belastung des Arbeitgebers kommen.

Möchte der Arbeitgeber einheitliche Spielregeln für alle Mitarbeiter schaffen, kann auch über eine Versorgungsordnung nachgedacht werden. Dies empfiehlt sich insbesondere für Unternehmen mit vielen Mitarbeitern und falls eine Unterscheidung zwischen bestimmten Personengruppen gewünscht ist (sofern diese sachlich begründet sind). Eine Versorgungsordnung beinhaltet klare Regeln für Arbeitgeberzuschüsse, den ausgewählten Durchführungsweg, Anbieter der betrieblichen Altersversorgung, Wartezeiten und sachliche Abgrenzungen von Personengruppen. Es besteht jedoch keine rechtliche Verpflichtung für die Erstellung einer Versorgungsordnung im Unternehmen. Eine gut ausformulierte und rechtlich einwandfreie Versorgungsordnung kann die Haftung des Arbeitgebers reduzieren, eine fehlerhafte oder nicht eindeutig formulierte Versorgungsordnung kann allerdings einen gegenteiligen Effekt haben. Aus diesem Grund sollte die Versorgungsordnung unter Beziehung rechtlicher Beratung erstellt und vorher genauestens geprüft werden.

31.3.3 Insolvenzsicherung

Ist ein Unternehmen zahlungsunfähig, zum Beispiel durch eine Insolvenz, so sind die Anwartschaften und Ansprüche auf betriebliche Altersversorgung unter bestimmten Voraussetzungen durch den Pensions-Sicherungs-Verein PVaG (PSVaG) geschützt. Dies trifft für die Durchführungswege Direktzusage, Unterstützungskasse, Pensionsfonds und auch (in relativen selten auftretenden Einzelfällen) für die Direktversicherung zu. In § 14 BetrAVG wird die Insolvenzsicherung über den Pensionssicherungsverein auf Gegenseitigkeit (PSVaG) beschrieben. Der Zweck dieser Einrichtung ist der Schutz von Leistungsbeziehern und Anwärtern mit Anspruch auf bAV. Geschützt werden gesetzlich unverfallbare Ansprüche auf bAV sowie laufende Rentenzahlungen. Der PSVaG wird durch die BaFin beaufsichtigt und durch die Kreditanstalt für Wiederaufbau (KfW) verwaltet. Im Falle einer Insolvenz des Arbeitgebers, der die Zusage gegenüber seinem Arbeitnehmer gegeben hat, übernimmt der PSVaG die Versorgung der entsprechenden Versorgungsberechtigten. Dies ist für die unmittelbaren Versorgungszusagen relevant, da durch eine Insolvenz des Arbeitgebers die zugesagten Leistungen nicht mehr erbracht werden können. Aus diesem Grund sind diese Formen der bAV sicherungspflichtig und der Arbeitgeber muss Beiträge an den PSVaG leisten. Bei mittelbaren Durchführungswegen (insbesondere in Form von Versicherung) entfällt die Beitragspflicht, da die Versorgungsansprüche durch die jeweilige Versorgungseinrichtung sichergestellt werden.

31.3.4 Vorzeitiges Ausscheiden von Arbeitnehmern

Für das Ausscheiden eines Mitarbeiters kann es neben einem Arbeitgeberwechsel unterschiedliche Gründe geben.

Seit dem 01.01.2018 gelten neue Regeln für die so genannte „Unverfallbarkeit“. Hiermit ist eine Regelung des § 1b BetrAVG gemeint. In dieser Vorschrift ist geregelt, was mit der zugesagten Anwartschaft passiert, wenn ein Mitarbeiter vorzeitig aus dem Unternehmen ausscheidet. Hierbei muss zwischen der Finanzierung durch Entgeltumwandlung und der Arbeitgeberfinanzierung unterschieden werden, denn eine Entgeltumwandlung ist immer sofort unverfallbar, wohingegen bei einer arbeitgeberfinanzierten Zusage dem Arbeitnehmer erst nach drei Jahren Betriebszugehörigkeit die Anwartschaft zuwächst. Dies gilt unter der Voraussetzung, dass der Arbeitnehmer das 21. Lebensjahr vollendet hat. Vor dem 01.01.2018 musste er das 25. Lebensjahr vollendet und das Dienstverhältnis mindestens für fünf Jahre bestanden haben. Bei dem neuen verpflichtenden Zuschuss des Arbeitgebers, der ja eigentlich arbeitgeberfinanziert ist, gibt es jedoch eine Sonderregelung. Der Zuschuss in Höhe von 15 Prozent des Entgeltumwandlungsbetrages ist ebenfalls sofort unverfallbar.

Scheidet ein Arbeitnehmer vorzeitig aus dem Unternehmen aus, wird der aus der Zusage begründete Anspruch durch vorgegebene Berechnungsverfahren begrenzt. Bei Direktversicherungen oder den versicherungähnlichen Pensionskassen kann neben dem ratierlichen Verfahren auch das versicherungsvertragliche Verfahren angewendet werden. Hierbei teilt der Arbeitgeber dem Versicherungsunternehmen oder der Pensionskasse mit, dass der Arbeitnehmer aus dem Unternehmen ausscheidet. Der Arbeitnehmer kann nun den Beitrag mit eigenen Beiträgen fortführen, den Vertrag beitragsfrei stellen oder bei einem neuen Arbeitgeber fortführen. Hierbei ist ein Urteil des Bundesarbeitsgerichtes vom 19.05.2016 zu beachten (BAG 3 AZR 794/14), durch das die Pflichten des Arbeitgebers verschärft wurden. Der Arbeitgeber muss dem Versicherungsunternehmen und dem Arbeitnehmer innerhalb von drei Monaten, nachdem er von dem Ausscheiden des Arbeitnehmers Kenntnis erlangt hat, mitteilen, dass das versicherungsvertragliche Verfahren (zur Anspruchsbegrenzung) angewendet werden soll.

31.3.5 Steuerung der bAV

Wie dargestellt, ist die bAV ein durchaus komplexes Thema in dem die Rechtsgebiete Arbeits-, Sozialversicherungs- und Steuerrecht zusammenwirken. Die professionelle Steuerung dieser Materie ist unerlässlich, um die positiven Effekte für den Arbeitgeber, aber auch um die Rechtsansprüche der Arbeitnehmer zu erfüllen. Grundsätzlich kommen drei Optionen in Betracht:

31.3.5.1 Eigene Steuerung

Je nach Betriebsgröße ist es möglich, die bAV unter anderem durch die eigene Personalabteilung steuern zu lassen. Kompetenz für die arbeits- und sozialversicherungsrechtliche Beurteilung kann hier grundsätzlich vorhanden sein. Auch die Beratung der eigenen Arbeitnehmer kann so durchgeführt werden, allerdings geschieht dies nicht „nebenbei“, da eine solche Beratung durchaus komplex und aufwendig sein kann. Es müssen daher ggf. spezielle Kapazitäten aufgebaut werden.

Bei der Einrichtung der bAV sind jedoch auch steuerrechtliche Fragen, zum Beispiel hinsichtlich der bilanziellen Auswirkungen, zu beantworten. Letztendlich muss der Durchführungsweg festgelegt werden und (bei einer mittelbaren Durchführung) muss zudem ein geeignetes Versorgungswerk/Versicherer gefunden werden. Dies kann im Regelfall nicht allein von der Personalabteilung bewerkstelligt werden.

31.3.5.2 Steuerung durch einen externen Dienstleister

Eine weitere Möglichkeit ist es, einen oder mehrere externe Dienstleister mit der Einführung der bAV bzw. auch mit der laufenden Beratung der Mitarbeiter zu beauftragen. In Betracht kommen hier spezialisierte Versicherungsvermittler sowie Steuerberater und ggf. Rechtsanwälte. Aber Vorsicht: Gerade wenn man mehrere Dienstleister ins Boot holt, müssen diese auch administriert, kontrolliert und vor allem bezahlt werden. Wenn der Versicherungsvermittler auch die Beratung der Mitarbeiter übernehmen sollte und zu diesem Zwecke Daten der Mitarbeiter zur Verfügung gestellt werden, muss hierfür eine datenschutzrechtliche Basis geschaffen werden. Positiv hervorzuheben ist sicherlich, dass diese Steuerung eine deutliche Entlastung der Ressourcen im eigenen Unternehmen bedeutet.

31.3.5.3 Steuerung durch einen konzern-eigenen fVV

Konzerne steuern ihre Versicherungsprogramme häufig über einen eigenen firmenverbundenen Versicherungsvermittler (fVV). Größtenteils sind diese fVV als GmbH organisiert. Zum einen stellt ein Konzern hiermit sicher, dass das Versicherungsmanagement in Konzerninteresse und mit eigenen Spezialisten durchgeführt wird, und zum anderen, dass erzielte Umsätze (mithilfe eines Beherrschungs- und Gewinnabführungsvertrags) an die Mutter abgeführt werden können.

Sofern der fVV neben den klassischen versicherbaren Konzernrisiken ebenso eine Kompetenz im Bereich der bAV vorhält, macht es natürlich Sinn, diese auch zu nutzen. Sowohl eventuelle Courtagen von Versicherungsgesellschaften als auch eine Dienstleistungsfee vom Konzern werden dann (wieder) an die Mutter zurückgeführt. Zudem werden sämtliche (eventuell vorhandene) Interessens- und Zielkonflikte beseitigt.

Die erforderliche Beratung der Mitarbeiter erfolgt dann auf kollegialer Basis, was mit einem erheblichen Vertrauensvorschuss verbunden ist und in der Regel eine höhere Durchdringung der bAV zur Folge hat.

Aufgrund der Integration des fVV in das Unternehmen und die damit verbundenen internen Kenntnisse, wie zum Beispiel Organisation, Historie etc., ist die Begleitung einer bAV auf diese Art weniger aufwendig.

Literatur

- Assekurata. (2016). ASSEKURATA Sondernewsletter 05/2016.
- Assekurata. (2019). ASSEKURATA-Marktstudie zu Überschussbeteiligungen und Garantien 2019. Köln.
- Bundesfinanzministerium. (2017). Gesetz zur Stärkung der betrieblichen Altersversorgung und zur Änderung anderer Gesetze (Betriebsrentenstärkungsgesetz). https://www.bundesfinanzministerium.de/Content/DE/Gesetzentexte/Gesetze_Verordnungen/2017-08-23-Betriebsrentenstaerzungsgesetz.html. Zugegriffen am 14.06.2019.
- Bundesministerium für Arbeit und Soziales. (2016a). Das Gesamtkonzept zur Alterssicherung. Berlin.
- Bundesministerium für Arbeit und Soziales. (2016b). Ergänzender Bericht der Bundesregierung zum Rentenversicherungsbericht 2016 gemäß § 154 Abs. 2 SGB VI (Alterssicherungsbericht 2016).
- Bundeszentrale für politische Bildung. (2019). <https://www.bpb.de/politik/innenpolitik/rentenpolitik/288929/3-saeulen-system-der-alterssicherung>. Zugegriffen am 03.09.2020.
- Buttler, A., & Keller, M. (2017). Einführung in die betriebliche Altersversorgung (8. Aufl.). Karlsruhe: VVW GmbH.
- Meissner, H., Kisters-Kölkes, M., Linden, R., & Friedrich, K. (2018). Leitfaden bAV: Betriebsrentenstärkungsgesetz (BRSG). Ein Kurzkommentar (3. Aufl.). Köln: Wolters Kluwer.
- Müller-Wirth, M. (2018). Arbeitnehmer: Was wünschen sich die Deutschen von ihrer Arbeit? ZEIT ONLINE, o. S. Zugegriffen am 13.12.2019.
- Sibinski, H., – Deutsche Rentenversicherung Bund. (2019). Studientext Nr. 40. Rechtsstand 2019 (23. Aufl.).
- Wissenschaftliche Dienste/Deutscher Bundestag. (2019). Grundlagen der betrieblichen Altersversorgung als zweite Säule der Alterssicherung in Deutschland, WD 6 – 3000 – 023/19.

Ingo Trosiner absolvierte zunächst eine Ausbildung zum Versicherungskaufmann bei der Barmenia Krankenversicherung aG. Von 2001 bis Juni 2020 war er bei der Deutsche Telekom Assekuranz-Vermittlungsgesellschaft mbH tätig. Zunächst als Leiter Krankenversicherung und dann seit 2012 als Bereichsleiter für das gesamte Privatkundengeschäft inklusive der bAV. Nebenberuflich studierte er Betriebswirtschaftslehre an der Steinbeis Hochschule Berlin sowie Wirtschaftsrecht an der Universität des Saarlandes. Seit Juli 2020 ist er bei der comdirect Versicherungsmakler AG als Vorstand verantwortlich für Produkmanagement und Vertrieb.

Dominik Hartmann arbeitet seit 2010 bei Swiss Life Select. Nach seiner Ausbildung zum Kaufmann für Versicherungen und Finanzen arbeitete er dort zunächst als Finanzberater und später zusätzlich als Spezialist für betriebliche Altersversorgung. Er studierte nebenberuflich Banking and Finance an der TH Köln (Bachelor) und im Anschluss nebenberuflich am Institut für Versicherungswesen der TH Köln Risk & Insurance (Master).



Projektmanagement und Projektversicherung

32

Lutz Torbohm und Svenja Schröder

Zusammenfassung

Das vorliegende Kapitel gibt einen Überblick über das Managen von Projekten und insbesondere über die möglichen Risiken und Schwierigkeiten bei der Zielerreichung dieser Projekte. Dabei werden die jeweiligen Risiken in verschiedene Risikogruppen unterteilt. Danach wird auf das Vermindern und Vermeiden dieser Risiken eingegangen und verschiedene Präventionsmechanismen dargestellt. Am Ende werden mögliche Versicherungslösungen und verschiedene Produkte beschrieben und erklärt, wobei die Versicherungssparten Bauwesenversicherung und Montageversicherung im Vordergrund der Betrachtung stehen. Ein Fazit und die Beurteilung von speziellen Projektversicherungen schließen das Kapitel ab.

32.1 Projektmanagement

Die Verknüpfung von Projektmanagements und Industriever sicherung ist ein komplexes und vielseitiges Thema. Dieses Kapitel soll hierzu Klarheit über die Zusammenhänge sowie über verschiedene Herangehensweisen schaffen. Im ersten Teil des Kapitels werden Definitionen über die Grundbegriffe des Projektmanagements und eine Übersicht über die zu beachtenden Risiken gegeben. Der zweite Teil des Kapitels baut die Brücke zum Thema

L. Torbohm

SMS Insurance GmbH, Düsseldorf, Deutschland

E-Mail: lutz.torbohm@sms-group.com

S. Schröder (✉)

TH Köln, Institut für Versicherungswesen, Köln, Deutschland

E-Mail: svenja.schroeder@hotmail.de

Industriever sicherung. Es wird dargestellt, wie die im Risikomanagement des Projektes identifizierten Risiken insbesondere mit den Sparten Bauwesenversicherung und Montageversicherung adäquat abgesichert werden können.

32.1.1 Definitionen

Im folgenden Abschnitt werden einleitende Definitionen und Erklärungen zu den Begriffen Projekt, Projektmanagement, Projektrisiken sowie Risikomanagement erarbeitet. Um sich im Nachfolgenden intensiv mit den Risiken und Herausforderungen eines Projektes befassen zu können, ist es von besonderer Wichtigkeit zu verstehen, wie ein Projekt strukturiert ist. Außerdem ist es wichtig klarzustellen, welche Parteien an einem Projekt beteiligt sind und wie diese mit eingebunden bzw. wie ihre Interessen beachtet werden müssen.

32.1.1.1 Projekt

Projekte gibt es überall, in allen Wirtschaftsbereichen, in allen Organisationen und für jede Person individuell. Gemäß der DIN Normenreihe 69901 ist das Hauptmerkmal eines Projektes die Einmaligkeit des Vorhabens. Die Einmaligkeit bezieht sich auf das Projektziel, die zeitlichen und finanziellen sowie personellen Begrenzungen in Verbindung mit der projektspezifischen Organisation (vgl. DIN 69901-5:2009-01, S. 11). Aus dieser Definition lassen sich folgenden zu erfüllenden Punkte ableiten:

- terminliche und sachliche Vorgaben sowie einzuhaltende Kosten,
- Einmaligkeit,
- interdisziplinäre Teamarbeit und arbeitsteilige Prozesse,
- Innovation.

Die Erfüllung eines Projektziels wird durch diese o. g. Punkte zu einem umfangreichen und intensiven Prozess, sodass ein adäquates Projektmanagement benötigt wird. Ein Projekt i. S. d. Kapitels liegt vor, wenn die Entscheidung zu einer Installierung eines Projektmanagers für ein konkretes Projekt getroffen wurde (vgl. Meyer und Reher 2016, S. 2–3).

32.1.1.2 Projektmanagement

Das Projektmanagement setzt sich typischerweise aus zwei Instanzen zusammen, der Projektleitung und der Projektsteuerung. Die Aufgaben dieser beiden Komponenten werden vom Bauherrn bzw. Auftraggeber eines Projektes unter Beachtung der den Projekterfolg beeinflussenden Faktoren bestimmt. Dies sind zum Beispiel Standort, Projektumfeld sowie projektspezifische Dinge. Es handelt sich bei dem Projektmanagement um eine einmalige Zusammensetzung; es ist also nur für ein Projekt bestimmt und somit können finanzielle, personelle und materielle Ressourcen zielgerichtet für das Projekt eingesetzt werden (vgl. Höllen et al. 2010, S. 19). Die an die beiden Instanzen delegierten Aufgaben orientieren sich an den Zielen des Projekts. So zählt die Anpassung von Spezifikationen,

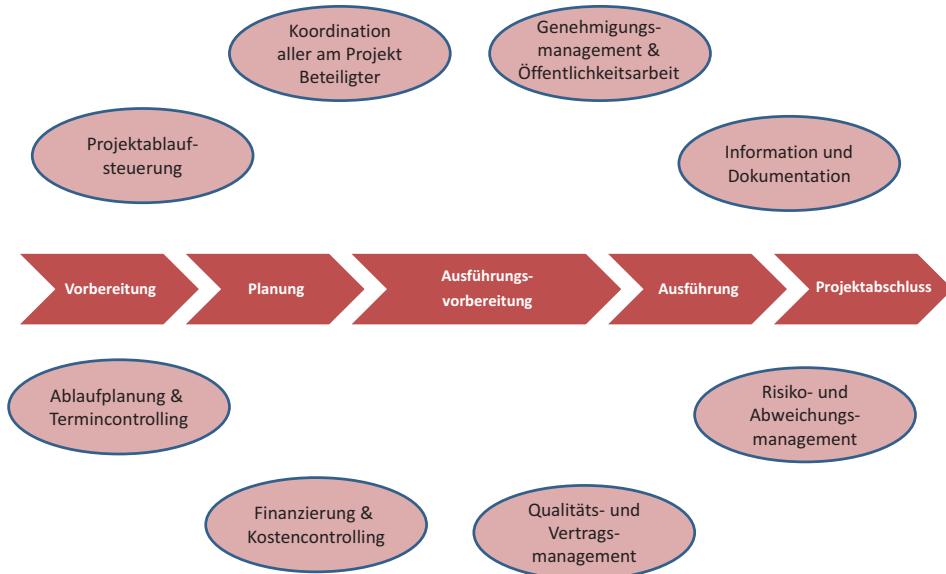


Abb. 32.1 Aufgaben des Projektmanagements. (Quelle: eigene Darstellung in Anlehnung an Höllen et al. 2010, S. 20)

Plänen und Vorgehensweisen an die jeweiligen Ansprüche der beteiligten Personen (Stakeholder) zu einer der wichtigsten Aufgaben. Dazu kommen die Definition realistischer Ziele und die dazugehörige Identifikation der Anforderungen. Das Planen von Fristen und Kosten, die qualitätsgerechte Lieferung der benötigten Gegenstände sowie am Ende die Verantwortung dafür, dass das Projekt zieltgerecht und mit einem wirtschaftlichen Erfolg abgeschlossen wird, vervollständigen das Aufgabenfeld (vgl. Meyer und Reher 2016, S. 3). Abb. 32.1 fasst alle Aufgaben des Projektmanagements während der Umsetzung zusammen und verdeutlicht den großen, zu beachtenden Umfang.

Die oben dargestellten Verflechtungen werden in Verträgen zum Projektmanagement einzelfallbezogen dokumentiert. Hier wird vertraglich vereinbart, welche konkreten Bedarfsanforderungen, steuerbare Vorgaben und auch nicht steuerbaren Rahmenbedingungen vorliegen. Außerdem werden die Ablauforganisation, der finanzielle Rahmen sowie der Terminrahmen festgelegt. Zusätzlich wird hiermit vertraglich festgeschrieben, in welchem Umfang die jeweiligen Instanzen Entscheidungen treffen dürfen und inwieweit sie die anderen Parteien informieren müssen (vgl. Höllen et al. 2010, S. 19). Ergänzt wird das Projektmanagement in der Regel durch einen Berater bzw. einen Projektsteuerer. Dieser stellt sicher, dass die Interessen des Bauherrn bei der Errichtung des Bauwerkes beachtet werden. Hierbei wird explizit auf die Übereinstimmung von der Planung mit der tatsächlichen Ausführung Wert gelegt. Außerdem wird eine Dokumentierung aller Aktivitäten vorgenommen.

32.1.1.3 Projektrisiken/Risikomanagement

Jede Ausführung eines Projekts geht mit einer Vielzahl von Risiken bzw. Gefahren einher, welche sich auf dem Weg zum Ziel in Form von Schäden, Verzögerungen oder sonstiger nachteiliger Form realisieren können und so die Erreichung des geplanten Projektziels gefährden können. Der Begriff Risiko wird in der Regel nicht einheitlich verwandt und daher im Rahmen dieses Kapitels in Abschn. 32.1.3.1 genau definiert. Wir sprechen zunächst von der Möglichkeit, dass ein negativer Ausgang einer Unternehmung mit möglichen Nachteilen, Verlusten und/oder Schäden eintreten kann. Die Folgen hieraus sind ungewiss, beeinflussen jedoch die Zielerreichung des Projektes (vgl. Brockhaus 2020). Um diese Risiken frühzeitig zu identifizieren und dementsprechend die Erreichung des Ziels zu schützen, benötigt jedes Projekt ein individuelles Risikomanagement. Eine Voraussetzung des Risikomanagements ist, eine „möglichst vollständige Erfassung aller Risikoquellen, von Schadenursachen sowie Störquellen“ (Romeike 2018, S. 9) zu gewährleisten. Dies geschieht mithilfe eines kontinuierlichen Prozesses, welcher in den vorherigen Kapiteln dieses Buches ausführlich beschrieben wurde. In Bezug auf das jeweilige Projekt besteht eine besondere Herausforderung darin, auch bei der Erfassung möglicher Risiken der Einmaligkeit eines Projekts gerecht zu werden.

32.1.2 Beteiligte Personen/Institutionen

Der folgende Abschnitt gibt einen Überblick über die unterschiedlichen Interessengruppen, welche an einem Projekt beteiligt sind. Jeder Bauherr bzw. jeder Verantwortliche für sowohl Risikomanagement als auch Projektversicherung sollte sich über den Umfang dieses Personenkreises bewusst sein. Aus diesem Grund wird folgend ein kurzer Überblick präsentiert.

32.1.2.1 Eigentümer, Bauherr, Initiator

Der Eigentümer, Auftraggeber oder auch Bauherr genannt, entwickelt die Idee des Projektziels und bedient sich zur Umsetzung dieser Idee anderer Unternehmen bzw. Dienstleister. Er verfolgt das Interesse, dass die Fertigstellung des Projektes ohne Überschreitung der Kosten frist- und qualitätsgerecht erfolgt (vgl. Ebner 2015, S. 40).

32.1.2.2 Architekt/Planer

Vor Beginn der Ausführung von Bau- bzw. Errichtungsarbeiten ist ein mehrstufiger Planungsprozess zu durchlaufen, der sowohl die Grundlage für die Ausschreibung der Gewerke als auch für die Einholung der erforderlichen Genehmigung darstellt. Vor Einleitung des Baubeginns muss zunächst ein Bauplan erstellt werden. Dieser geht durch verschiedene Instanzen, wie zum Beispiel unter Einbeziehung eines Architekten oder eines Statikers. Auch diese Personen sollten in das Projektmanagement aufgenommen werden, da sie entscheidende Aufgaben bzw. Teilaufgaben eines Projektvorhabens ausführen. Demzufolge kann die Erfüllung dieser Aufgaben großen Einfluss auf die Erreichung des

Projektziels haben bzw. das Risiko des Nichterreichens der entsprechenden Teilziele des Projekts oder das Gesamtziel gefährden.

32.1.2.3 Ausführende Unternehmen

Die Ausführung der verschiedenen Schritte bzw. Maßnahmen, die zur Realisierung des geplanten Objektes getroffen werden müssen, werden dementsprechend von einem beauftragten Unternehmen durchgeführt. Hierbei kann es sich selbstverständlich um verschiedene Unternehmen handeln. Man spricht auch vom Auftragnehmer und seinen verschiedenen Subunternehmern.

32.1.2.4 Anwohner, Anlieger, Öffentlichkeit

Sowohl die Umgebung der Baustelle als auch die Art des Bauprojektes selbst bzw. die Kombination aus beiden stellen wichtige Aspekte des Projektmanagements dar. Durch Beschwerden oder sogar Klagen kann das Bauvorhaben unterbrochen oder erschwert werden.

32.1.3 Risiken eines Projektes

Die Identifikation der Risiken eines Projektes macht es erforderlich, dass ein Großteil der zuvor genannten beteiligten Personen in das Risikomanagement eines Projektes einbezogen werden müssen, um sicherzustellen, dass Risiken in allen beteiligten Bereichen Berücksichtigung finden. Das Erreichen des definierten Projektziels kann durch unterschiedliche Risiken gefährdet werden. Da hierbei nicht jedes Risiko ein projektspezifisches Risiko darstellt, wird im Folgenden eine Einteilung in allgemeine Risiken und spezifische Risiken für ein bestimmtes Projekt vorgenommen. Im Anschluss daran werden die Risiken dargestellt, welche im Projektverlauf einen Haftungsanspruch anderer Parteien hervorrufen können. Des Weiteren wird in einem vorgelagerten Absatz kurz auf die Risikoanalyse sowie auf die Begrifflichkeiten „Risiko“ und „Gefahr“ eingegangen.

32.1.3.1 Risikoanalyse

Die Risikoanalyse setzt sich zusammen aus der Identifikation und der Bewertung von Risiken, welche während eines Prozesses eintreten können. Eine sorgfältige Analyse führt zu einem besseren und günstigeren Verlauf eines Projektes und gehört daher, wie in Abschn. 32.1.1.1 erläutert, zu den Aufgaben des Risikomanagements. Klar zu trennen sind die Begrifflichkeiten Gefahr und Risiko. Bei einem Risiko sprechen wir von einer unsicheren Zukunftssituation, bei der es Wahrscheinlichkeitsaussagen über das Eintreten bestimmter Zustände in der Zukunft gibt. Es besteht also eine Gewissheit darüber, dass ein bedrohliches Ereignis, welches das Projekt gefährden könnte, eintreten wird. Vorhersehbare Umwelteinflüsse mit einer bestimmten Eintrittswahrscheinlichkeit definieren demnach das Risiko. Versicherungstechnisch kommt noch eine weitere Komponente hinzu, nämlich die Schadenhöhe. Hier lautet die genaue Definition: Eintrittswahrscheinlichkeit multipliziert

mit der Schadenhöhe ergibt das versicherungstechnische Risiko (vgl. Nguyen 2007, S. 95). Auch der Begriff Gefahr könnte in diesem Zusammenhang umgangssprachlich verwendet werden. Er beschreibt die Möglichkeit, dass es zu einem Schaden bzw. einem negativen Ereignis kommt. Da der Begriff Risiko in der Versicherungspraxis allerdings den gebräuchlicheren Begriff darstellt, wird dieser im Verlauf dieses Kapitels benutzt.

32.1.3.2 Allgemeine Risiken für ein Projekt

Neben den projektspezifischen Risiken müssen allgemeinen Risiken berücksichtigt werden. Sie bestehen nicht speziell für ein konkretes Projekt, sondern sind grundsätzlich vorhanden und können die Zielerreichung gefährden. Die Eintrittswahrscheinlichkeit der Risiken ist je nach Projektort unterschiedlich.

Naturrisiken

Naturrisiken bezeichnen Ereignisse in der Natur, die zu einer Bedrohung des Projektvorhabens führen können. „Praktisch die gesamte Erdoberfläche ist in irgendeiner Form von Naturgefahren betroffen, schadenverursachende Ereignisse treten allerdings – in Abhängigkeit der spezifischen Gefahrendisposition und des Schadenpotenzials einer Region – mit unterschiedlicher Häufigkeit und Intensität in Erscheinung“ (Rudolf-Miklau und Suda 2012, S. 1). Diese Aussage untermauert die große Bedeutung von Naturrisiken und zeigt in diesem Zusammenhang das enorme Risikopotenzial.

Unterschieden wird zwischen Naturgefahren mit globaler Bedeutung, die also großflächige Auswirkungen aufweisen, wie zum Beispiel Stürme oder Hochwasser, und Naturgefahren, welche nur lokal wirken, wie zum Beispiel Lawinen (vgl. Rudolf-Miklau und Suda 2012, S. 2). Die Standortwahl hat also einen direkten Einfluss auf das Projekt.

Wirtschaftspolitische Risiken

Zinsschwankungen und andere Risiken aus dem Finanzmarkt fließen ebenfalls in die Planung eines Projektes mit ein. Je nach Errichtungsort sind Währungsrisiken und Zahlungsrisiken von Bedeutung.

Allgemeine Compliance Risiken

Der gesetzliche Ordnungsrahmen setzt sich unabhängig von dem im Projektvertrag geregeltem Recht zwischen Auftraggeber und Auftragnehmer zusammen. Vielmehr orientiert er sich an dem Ort, an dem das Projekt gestaltet und durchgeführt wird, also dem Errichtungsort. Zu beachten sind die örtlichen Regelungen des Arbeits- und Sozialversicherungsrechts, Börsen- und Kapitalmarktrechts, Exportkontrolle und Außenwirtschaftsrechts, Gesellschaftsrechts, Kartellrechts, Steuerrechts, Umweltrechts etc. sowie Regelungen zu den insolvenzrechtlichen Haftungsfragen und der versicherungsrechtlichen Aufsichtsbehörde (vgl. Umnuß 2017).

Cyber-Risiken

Die Ausführung eines Projektes wird heute von zahlreichen digitalen Prozessen und dem Einsatz digitaler Tools begleitet bzw. unterstützt. Bei der Installation von Elektrik- und Automationssteuerungen sowie Software-Modulen sind datentechnische Schnittstellen zu vorhandenen Systemen bzw. zwischen Systemen verschiedener Gewerke zu berücksichtigen. Auch die Gefahr der Manipulation von IT-Systemen von außen durch Dritte oder die Verletzung datenschutzrechtlicher Bestimmungen bergen Risiken für ein Projekt (vgl. Torbohm 2018, S. 4).

Risiken der Wirtschaftskriminalität

Je nach Errichtungsort können Risiken aus Wirtschaftskriminalität eine mehr oder weniger große Bedeutung haben. Zu beachten sind hier Szenarien wie zum Beispiel Betrug, Raub oder Diebstahl bis hin zu Erpressungen und Entführungen.

Politische Risiken

Themen wie Krieg oder Terror sind gesondert zu berücksichtigen, da sie meist gar nicht oder nur schwer abzusichern sind. Deswegen liegt hierbei eine besondere Risikokategorie vor, sie sollte aber in der Projektplanung Beachtung finden. Auch unter diesen Punkt fallen zum Beispiel Streik, Aufruhr und politische Risiken.

32.1.3.3 Spezifische Risiken für Projekte

Folgend werden die Risiken behandelt, die im direkten Zusammenhang mit der Durchführung des Projektes stehen. Sie entstehen im Verlauf dieses Prozesses und müssen je nach Projektvorhaben individuell identifiziert und separat behandelt werden.

Risiken am Errichtungsort/aus der Montage

Während der Arbeiten auf der Baustelle kann es zu mechanischem Versagen von Bauteilen, Werkzeugen, Betriebsmitteln oder auch Transportmitteln kommen. Dieses kann durch einfache Arbeiten aus der Montage heraus oder durch andere Einflüsse geschehen. Die Nachlieferung oder Reparatur kann oft einige Zeit in Anspruch nehmen und führt daher zu beachtlichen Kosten- und Zeiträumen. Hinzu kommen geologische Risiken sowie Risiken aus der unmittelbaren Lage eines Standorts (zum Beispiel am Fluss, Meer, im Lawinenbereich usw.).

Risiken betreffend Versorgungsleistungen/Infrastruktur am Errichtungsort

Für den Bauprozess während eines Projektes werden Ressourcen zum Betrieb der Arbeiten benötigt. Hierunter fallen Komponenten wie Strom/Elektrizität, Wasser, Druckluft sowie ein funktionierendes IT-Netz. Daneben ist natürlich auch die allgemeine Infrastruktur am Errichtungsort, welche erforderlich ist um Baumaterial, Hilfsstoffe, Maschinen und Personal termingerecht zu den geplanten Kosten verfügbar zu haben, unumgänglich. Im Umkehrschluss bedeutet dies, dass ohne eine funktionierende Infrastruktur das Projektvorhaben gefährdet wird und daraus entsprechende Risiken entstehen können.

Risiken im Bereich Performance

Für einen reibungslosen Ablauf eines Projektes sind unmittelbar die ausführenden Personen verantwortlich. Da jedoch immer auch menschliches Versagen bzw. menschliche Fehler mitberücksichtigt werden müssen, spielt die Performance dieser Personen eine kritische Rolle. Beispiel hierfür sind Anlagen oder Gebäude, bei denen im Rahmen der Inbetriebnahme offenkundig wird, dass die vertraglich geschuldete Leistung/Kapazität des Projektgegenstandes nicht erreicht wird aufgrund von mangelnder Planung und/oder Ausführung des Projektes.

Transportrisiken

Unter das Transportrisiko fallen der vollständige oder anteilige Verlust von Bauteilen und Material oder deren Beschädigung. Unterschiedliche Transportwege und Transportmittel stellen verschiedene Risiken dar, welche volumänglich in der Projektplanung berücksichtigt werden müssen. Eine größere Beachtung gilt Bauprojekten auf dem Wasser (offshore). Hier besteht ein besonders hohes Risiko während der verschiedenen Transporte, welches mit höheren Kosten verbunden sein kann. Bei Transportrisiken ist von großer Bedeutung, auf wessen Risiko ein Transport einer Sache erfolgt und an welchem Ort der Risikoübergang zwischen Lieferanten und Empfänger vereinbart wird sowie welche Partei Versicherungsschutz bereitstellen muss (gemäß Incoterms). Auch wenn Transportrisiken häufig primär den Lieferanten oder Besteller (in der Regel Auftragnehmer) tangieren, können sie Verzögerungen im Projektlauf verursachen und die termingerechte Fertigstellung eines Projektes gefährden.

Risiken bei der Inbetriebnahme bzw. im Probebetrieb

Jedes Projekt wird mit einem Probeflug abgeschlossen. Dieser Probeflug nimmt besonders im Anlagenbau eine wichtige Rolle ein, wohingegen er beim Gebäudebau etwas weniger zum Tragen kommt. Trotzdem muss hier durch eine Erprobung belegt werden, dass das Gewerk mit dem Planvorhaben übereinstimmt. Der Probeflug schließt sich direkt an die erstmalige Inbetriebnahme der erbauten Anlage bzw. des fertiggestellten Projektes an und in seinem Verlauf muss der Nachweis darüber erbracht werden, dass die im Projektvertrag vereinbarte Projektspezifikation erfüllt wird. Wird der Probeflug erfolgreich beendet, so ist das Projekt offiziell abgeschlossen. Die Zeitspanne für den Probeflug variiert je nach Art und Größe des Projektes und kann unter Umständen mehrere Monate in Anspruch nehmen.

Vertragliche Risiken

In einem Projekt gibt es eine Vielzahl unterschiedlicher Vertragsbeziehungen. Vom Auftraggeber bis hin zum letzten Subunternehmen bzw. Lieferanten sind alle am Projekt beteiligten Personen vertraglich miteinander verbunden, jedoch nicht immer in Form direkter Vertragsbeziehungen. Ein funktionierendes Vertragsmanagement sollte berücksichtigen, in welcher Form und in welchem Umfang vertraglichen Pflichten an Nachunternehmer weitergegeben werden; entsprechende vertragliche Vorgaben sind hier

erforderlich. Auch muss sichergestellt werden, dass zwischen Vertragsparteien geschlossene Vereinbarungen rechtssicher zustande gekommen (AGB- und auslegungssicher) und in sich konsistent gestaltet sind (zum Beispiel Schlüssigkeit der Ausgestaltung vertraglicher Haftungs-, Entschädigungs- sowie damit korrespondierender Versicherungsbestimmungen).

Konformitätsrisiken

Für jedes Bauwerk oder technisches Gewerk sind die einschlägigen Sicherheits- sowie Brandschutzzvorschriften und alles sonstigen technischen Vorschriften für die Bauwerks- bzw. Anlagensicherheit einzuhalten. Werden diese nicht ordnungsgemäß eingehalten, kann es zu Baustopps oder anderen Verzögerungen, bis hin zu einer Verweigerung der Abnahme des Projektes kommen.

32.1.3.4 Haftungsrisiken durch ein Projekt

Risiken aus Gewährleistung/Performance

Unter Gewährleistungshaftung, auch Mangelhaftung genannt, versteht das deutsche Schuldrecht das „Einstehen müssen“ für eine **mangelhafte** Leistung. Die Haftung für Sach- und Rechtsmängel steht hierbei im Vordergrund. Mängel entstehen meistens aus einer nicht korrekt ausgeführten Leistung. Dies kann sowohl in einem Mangel bzw. Fehler in der Planung als auch in der Ausführung der Arbeiten zur Errichtung des Projektes begründet sein. Aus Sicht des Auftraggebers ist es wichtig, dass die beauftragten Unternehmen über einen entsprechenden Versicherungsschutz zur Absicherung von Gewährleistungs- und Performancerisiken verfügen.

Risiken durch zivilrechtliche, verwaltungsrechtliche und strafrechtliche Konsequenzen

Neben Fehlern auf der Baustelle sind sowohl Ansprüche unter den Beteiligten als auch von Dritten (nicht aktiv am Projekt Beteiligten) zu berücksichtigen. Ein wichtiger Punkt sind auch die durch Fehler während des Projektes betroffenen Verwalter, Immobilienmakler, Facility-Manager, Dienstleister etc. Zu guter Letzt sind auch die Investoren zu berücksichtigen, welche als Geldgeber des Projektes ein finanzielles Ausfallrisiko tragen und Entschädigungen von Vertragspartnern fordern können (vgl. Ebner 2015, S. 41).

Risiken durch die Inbetriebnahme bzw. den Probebetrieb

In Abschn. 32.1.1.3 wurde auf die Thematik des Probebetriebs bereits eingegangen. Dabei liegt während dieser Zeit die Verantwortung für das erbaute Objekt weitgehend beim Auftragnehmer, da ein Eigentumsübergang an dem zu errichtenden Bauwerk/Projektgegenstand noch nicht vorliegt (eine Abnahme des Projektes ist noch nicht erfolgt). Jedoch ist zu berücksichtigen, dass auch Dritte durch bzw. im Zusammenhang mit der Inbetriebnahme bzw. einem Probeflug geschädigt werden können und dies sowohl Schadenserstattungsansprüche gegen den Auftragnehmer als auch gegen den Auftraggeber bzw. im Sinne einer Gesamtschuld gegen beide begründen können (vgl. Torbohm 2018, S. 4).

32.1.4 Konsequenzen für das Projekt

Nachdem ein umfassender Überblick über wichtige Faktoren, welche dem Projektziel im Weg stehen können, erbracht wurde, geht es nun um die möglichen Folgen. Hierbei wird zwischen den potenziellen Risiken und den daraus resultierenden Konsequenzen unterschieden. Die im Vordergrund stehende Folge aus allen oben genannten Risiken ist die Gefährdung des Projektvorhabens. Dabei sind drei Szenarien hervorzuheben: Das Projekt wird teurer als geplant, das Projekt dauert länger als geplant oder das Projektergebnis weist mangelnde Qualität auf. Diese Szenarien treten oft in Kombination miteinander auf, sodass es zu besonders kritischen Situationen kommen kann. Wie dagegen vorgegangen werden kann bzw. welche Konsequenzen daraus resultieren, wird in den folgenden Abschnitten beschrieben. Zur besseren Abgrenzung wird im Folgenden eine Einteilung in vermeidende, präventive und vermindernde Maßnahmen getroffen.

32.1.4.1 Vermeidung

Um verschiedene Risiken grundsätzlich zu vermeiden, wird in der Projektplanung abgewogen, ob es einen weniger risikoreichen Weg gibt. Ein gutes Beispiel hierfür ist die Standortwahl. Werden hier bzgl. der Öffentlichkeit, Nähe zu stark besiedelten Städten oder auch aufgrund möglicher Naturgefahren große Risiken gesehen, sollte sich das Projektmanagement die Frage stellen, ob es einen geeigneteren Ort für das Projekt gibt. So können spezielle Risiken von Anfang an vermieden werden. Erst wenn es keine andere Möglichkeit gibt, ist über Maßnahmen der Prävention oder der Verminderung nachzudenken.

32.1.4.2 Prävention

Drohenden Gefahren bzw. identifizierten Risiken kann sowohl mit technischen Maßnahmen als auch mit vertraglichen Maßnahmen begegnet werden, wenn gleich durch beide Maßnahmen nur in seltenen Fällen eine vollständige Eindämmung einer Gefahr erreichbar ist. Bei Schwierigkeiten bzgl. der öffentlichen Akzeptanz und/oder der Genehmigungsfähigkeit eines Projektes stellt eine offene und professionelle Kommunikation unter Einbeziehung der vorgenannten Maßnahmen eine Möglichkeit dar, Störungen im Projektablauf präventiv entgegen zu wirken.

Technische Prävention betrifft Maßnahmen, welche sowohl durch digitale Tools als auch durch technische Vorkehrungen eingeleitet werden können. Hier können zum Beispiel Sensoren, Detektoren oder andere Hilfsmittel zum Einsatz kommen, welche frühzeitig zu erkennen helfen, dass sich bestimmte Risiken entwickeln. Somit kann früh genug gegen die Realisierung des Risikos angegangen werden. Das Projektmanagement kann dementsprechend die verantwortlichen Unternehmen vertraglich verpflichten, entsprechende Hilfsmittel in ihre technische Planung von Beginn an einzubeziehen.

Hinsichtlich der vertraglichen Maßnahmen zur Prävention sind die unterschiedlichen Vertragsmodelle zu beachten. Im Anlagenbau gibt es zum Beispiel das Vertragsmodell „EPC-Generalunternehmer“ (Engineering, Procurement, Construction), bei dem der

Vertrag zwischen dem Auftraggeber und dem Generalunternehmer geschlossen wird. Dem Generalunternehmer obliegt hierbei die Auswahl, Einbindung und Überwachung der eingebundenen Lieferanten sowie der Unterlieferanten. Dahingegen gibt es das „EPC-Konsortium“, wobei der Vertrag zwischen einem Konsortium und dem Auftraggeber geschlossen wird. Hierbei werden die Verantwortlichkeiten geteilt und in einem Kooperationsvertrag zwischen den Konsorten festgelegt. Der Generalunternehmer trägt die Verantwortung für den Erfolg des Projektes gegenüber dem Auftraggeber selbst (vgl. Torbohm 2018, S. 4–5). Die verschiedenen Vertragsmodelle werden von Projektart zu Projektart anders benannt und definiert. Die grundlegenden Fragen bleiben dabei gleich: Mit wem geht der Auftraggeber ein Vertragsverhältnis ein? Gibt es einen Vertrag mit dem Generalunternehmer oder gibt es mehrere einzelne Verträge mit Gesellschaften und Subunternehmen? „Die vertragliche Situation ist so beschaffen, dass eine Vertragspartei (die Auftraggeberseite) die andere Vertragspartei (die Auftragnehmerseite) für die Realisierung des Projekts vergütet und folglich auch ohne weiteres im eigenen Namen gegen den Auftragnehmer Rechte wegen Nicht- oder Schlechterfüllung geltend machen kann“ (Ensthaler et al. 2012, S. 329). Diese Aussage zeigt die Wichtigkeit des Vertragsmanagements in einem Projekt.

Bei der Vertragsgestaltung sollte bei einigen Konstellationen besondere Aufmerksamkeit gelten. So ist zum Beispiel zu beachten, dass bei der Vertragsgestaltung mit Planern, zum Beispiel Architekten, zum einen die „vollständige Prüf-, Beurteilungs- und Darstellungspflicht einschließlich damit verbundener Kosten zum Beispiel für Dateneinkauf bei Dritten und zum Anderen die nicht sichere Vorhersehbarkeit geologischer und hydrologischer Verhältnisse im Feld und im Zielhorizont“ (Höllen et al. 2010, S. 91) zu berücksichtigen sind.

Ein weiterer präventiver Schritt ist die Zusammenarbeit mit den Anwohnern und der Öffentlichkeit. In diesem Zusammenhang spielt eine angemessene und konstruktive Kommunikation mit dem Projektumfeld eine wichtige Rolle. Eine mögliche Lösung kann zum Beispiel sein, die Bürger in die Entscheidungen und in die Planung mit einzubeziehen und sie dadurch zu einem Teil des Projektes werden zu lassen. Hierbei sind drei Aspekte zu beachten: Der gesellschaftliche Aspekt verlangt, dass es, nachdem ein Projekt beschlossen und genehmigt wurde, keine Widersprüchlichkeiten oder Verzögerungen geben darf. Haben die Bürger einmal ihre Akzeptanz für das Vorhaben gegeben, müssen die Erwartungen und Vereinbarungen eingehalten werden, damit es nicht zu Streitigkeiten kommen kann. Der zweite Punkt betrifft den genehmigungsrechtlichen Aspekt. Der Weg bis zur Genehmigung eines Projektes kann durch mehrere Instanzen führen. Während dieses Ablaufs ist zu beachten, dass alle Kritikpunkte, welche zu einer Ablehnung des Projektes führen können, offen kommuniziert werden. Der Öffentlichkeit sollten also keine Fakten vorenthalten werden, damit es im Nachhinein keinen Anlass für Unmut und daraus folgend genehmigungsverzögernde oder -verhindernde Einflüsse gibt. Als letzter Aspekt ist die allgemeine Kommunikation zu nennen. Die Stichpunkte Information und Transparenz sind hierbei ausschlaggebend. Es geht um eine frühzeitige, kontinuierliche und persönliche Information der Betroffenen. Um ihr Vertrauen nicht zu verlieren, sollten alle

Änderungen, Neuerungen und Abweichungen vom ursprünglichen Plan transparent offengelegt werden (vgl. Hofmann und Sinemus 2013, S. 143–144).

32.1.4.3 Verminderung

Gibt es keine Möglichkeit, trotz bedrohenden Gegebenheiten am Errichtungsort, einen anderen Standort zu wählen, können andere Maßnahmen getroffen werden. Befindet sich der Errichtungsort zum Beispiel nah an einem Fluss, könnte mithilfe von Schutzmauern o. ä. einer möglichen Überflutung entgegengewirkt werden.

Für den Fall, dass ein Schadenereignis trotz oben genannter Vorsichtsmaßnahmen eintritt, gibt es verschiedene Wege, die Auswirkungen zu reduzieren. Im Abschn. 32.1.2 wird auf die Möglichkeiten durch einen adäquaten Risikotransfer eingegangen und somit die Brücke zur Industriever sicherung gebaut.

32.2 Versicherungsformen

Im Zweiten Teil dieses Kapitels geht es um die versicherungstechnische Absicherung von Projekten und im speziellen um die Risiken während der eigentlichen Bauphase. Unterteilt wird dieser Teil in die Absicherung von Risiken für ein Projekt selbst und die Haftungsrisiken, die aus einem Projekt hervorgehen können.

Es gibt grundsätzlich zwei verschiedene Arten, wie ein Projekt über Versicherung abgesichert werden kann.

Die eine Möglichkeit ist, Projektrisiken im Rahmen vorhandener Jahresverträge mitzuversichern, also ohne separate, eigenständige Projektversicherungen zu installieren. Abhängig von den betrieblichen Tätigkeiten des Bauherrn können hier jedoch inhaltlich signifikante Erweiterungen erforderlich werden, die sich darüber hinaus auch in separaten, zusätzlichen Prämien niederschlagen können. Auch wird hierbei regelmäßig eine Erweiterung des Kreises der versicherten Personen bzw. Unternehmen, die in den Versicherungsschutz mit einzubeziehen sind, erforderlich. Wird hingegen auf die bestehenden Versicherungen eines Generalunternehmers oder Konsortialführers zurückgegriffen, sollte der Deckungsumfang grundsätzlich weniger Anpassungen erfordern, jedoch ist eine Vereinbarung zur Einbeziehung des Auftraggebers und seiner Interessen aus der Ausführung des Projektes erforderlich.

Die zweite Möglichkeit ist, eine separate, nur für das eine Projekt geltende Projektversicherung abzuschließen. Im weiteren Verlauf dieses Kapitels wird diese Möglichkeit einer separaten Projektversicherung näher beleuchtet, die für alle am Bau/Projekt beteiligten Unternehmen abgeschlossen wird. Auch diese Form der Absicherung hat verschiedene Vor- und Nachteile, welche ausführlich benannt und analysiert werden. Hierbei geht es im Wesentlichen um die Risiken, die während der Bauphase eines Projektes, vom Baubeginn bis zur Bauabnahme, bestehen. Dabei wird keine vollständige Analyse aller zu versicherten Gegebenheiten vor, während und nach einem Projekt vorgenommen. Vielmehr konzentrieren sich die folgenden Ausführungen auf Projekte in Deutschland im Bereich Hoch- und Tiefbau und im Anlagenbau.

32.2.1 Projektversicherung

Bei der Projektversicherung beschränken sich der komplette Vertrag und insbesondere auch die Versicherungssumme, auf ein konkretes Projekt. Der Vertrag ist also explizit für ein Projekt abgeschlossen und sichert keine weiteren Projekte mit ab. Die Laufzeit des Vertrages beschränkt sich auf den Zeitraum, in dem das Projekt abgewickelt wird, also vom Planungsbeginn bis zur Abnahme des Projektes. Eine Projektpolice ermöglicht es somit, eine adäquat an die Gegebenheiten angepasste Lösung zu erstellen und überflüssige Deckungen zu vermeiden sowie spezielle Einschlüsse zu berücksichtigen. Dies bedeutet zwar einen höheren einmaligen Aufwand hinsichtlich der Risikoprüfung, führt aber am Ende zu einer genauen und umfassenden Absicherung der Projektrisiken.

Ein Hauptbestandteil einer Projektpolice ist die Bauleistungsversicherung, welche der Absicherung des Eigenschadens während des Bau- bzw. Montageprozesses dient. Zusätzlich wird gezielt eine passende Haftpflichtlösung für das konkrete Projekt ausgewählt und abgeschlossen. Als zusätzliche Deckungsbausteine können Transportrisiken sowie Unterbrechungsrisiken eingeschlossen werden. Beim Abschluss einer Projektversicherung können spezielle Anforderungen adressiert werden, wie zum Beispiel die vollständige Mitversicherung des Arbeitsgemeinschafts-Partners sowie der Subunternehmer oder eine separat zur Verfügung stehende Deckungssumme für diese Beteiligten. Diese Anforderungen können oftmals vom vorhandenen Versicherungsschutz nicht erfüllt werden.

Abb. 32.2 und 32.3 vermitteln einen Überblick über benötigte Versicherungssparten. Die Transportversicherung wird im Folgenden nicht weiter erörtert.

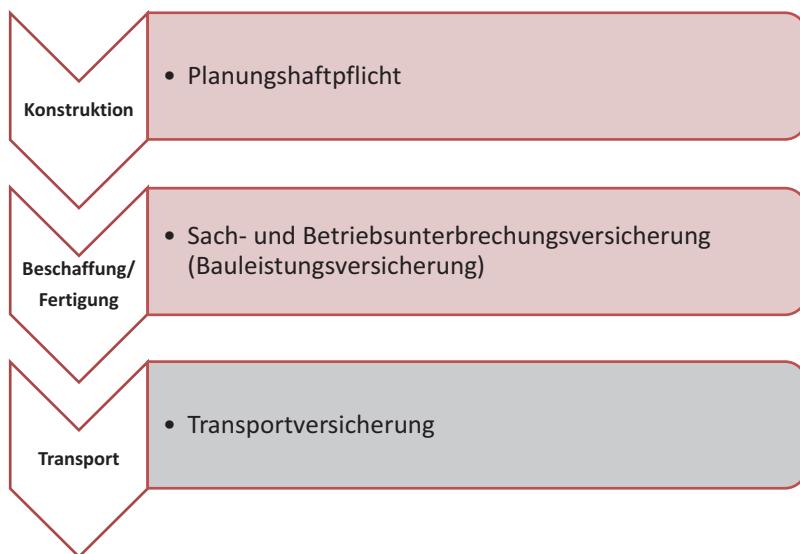


Abb. 32.2 Übersicht der Versicherungen außerhalb des Errichtungsortes. (Quelle: eigene Darstellung)



Abb. 32.3 Übersicht der Versicherung am bzw. auf dem Errichtungsort. (Quelle: eigene Darstellung)

Folgende Fragen müssen vor Abschluss einer Projektversicherung beantwortet werden:

- Wessen Interessen sollen neben denen des Versicherungsnehmers versichert werden?
- Welche Vertragsdauer ist für eine Projektversicherung nötig?
- Wer zahlt die Prämie?
- Wer trägt im Falle eines Schadens die Selbstbeteiligung?

Diese Fragen bzw. deren Antworten werden im Projektvertrag zwischen Auftraggeber und Auftragnehmer festgelegt. Hierbei gibt es verschiedene Konstellationen, wobei darauf geachtet werden muss, dass alle Interessen, sowohl auf Auftraggeber- als auch auf Auftragnehmerseite, adäquat abgesichert werden.

Im Weiteren wird von der Konstellation ausgegangen, dass der Auftraggeber für die Absicherung des Projektes zuständig ist. Der Auftraggeber schließt für alle am Projekt beteiligten Personen und Unternehmen eine Projektdeckung ab. Herauszunehmen sind hier allerdings die Unternehmen, welche ihre Arbeit nicht am Errichtungsort verüben, sondern ausschließlich als Lieferanten für den Auftragnehmer fungieren. Da es sich hier um ein reines Liefergeschäft handelt, steht grundsätzlich eine Absicherung für Haftungsrisiken aus dem Liefergeschäft über die Betriebs- und Produkthaftpflichtversicherung des Lieferanten zur Verfügung. Das kann insbesondere bei langen Projektzeiträumen zu folgender Problematik führen: Der Auftragnehmer hat ein Gewährleistungsrecht bei seinem Lieferanten und muss gegenüber seinem eigenen Auftraggeber für seine Arbeiten haften. Hierbei sind die verschiedenen Fristen von großer Bedeutung. Die Fristen beginnen zu unterschiedlichen Zeitpunkten. So startet die Gewährleistungspflicht des Auftragnehmers gegenüber dem Auftraggeber mit Fertigstellung des Projektes, die Gewährleistungsfrist des Lieferanten gegenüber dem Auftragnehmer jedoch mit dem Lieferungsdatum, welches sich innerhalb der Projektzeit befindet. Der Auftragnehmer muss diesbezüglich entsprechende Regelungen mit seinem Lieferanten festhalten, um dieser Gefahr aus dem Weg zu gehen. Eine weitere Möglichkeit ist, dieses Risiko in die Versicherungsverträge des Auftragnehmers mit einzuschließen bzw. das Risiko aus einem solchen Liefergeschäft mit in die Projektversicherung als eigenes versichertes Interesse mit aufzunehmen.

Eine weitere Konstellation könnte zum Beispiel sein, dass der Auftragnehmer die Projektversicherung abschließt. Diese Konstellation wird im Umfang dieses Kapitels nicht weiter erläutert.

32.2.1.1 Versicherung für allgemeine und projektspezifische Risiken eines Projekts

Bei einer Projektversicherung im Sinne dieses Kapitels geht es um die Absicherung von Schäden am Leistungs- und Liefergegenstand für das Projekt sowie um Schäden durch den Leistungs- und Liefergegenstand bzw. im Zusammenhang mit der Ausführung der Projektarbeiten. Schäden am Leistungs- und Liefergegenstand stellen vor Eigentums- und Risikoübergang bis zum Zeitpunkt der Objektabnahme einen Eigenschaden für das bauausführende Unternehmen dar. Dieses trägt bis zur Fertigstellung des Baus die Verantwortung für den reibungslosen Projektablauf und kann auch im Sinne der Nachhaftung in Anspruch genommen werden. Hierunter können Sachschäden fallen, aber auch daraus folgende Vermögensschäden durch eine Verzögerung in der Fertigstellung des Baus. Der Schaden, der durch eine solche Verspätung entsteht, ist mehr oder weniger ausschlaggebend für die verschiedenen Baubeteiligten. So muss zum Beispiel der Auftraggeber (Bauherr) Mietzusagen fristgemäß einhalten und der Auftragnehmer muss seinen Planungen bzgl. Gerätschaften und Personal erfüllen (vgl. Thevis 2018). Hierbei ist bei der Versicherungswahl darauf zu achten, in wieweit diese Vermögensschäden über die Projektversicherung für Versicherungsnehmer sowie für die mitversicherten Unternehmen mit eingeschlossen sind.

Im Folgenden wird kurz auf die beiden angekündigten Projektformen Bau und Montage näher eingegangen.

Contractor's All Risk (CAR)

In CAR-Policen geht es um die Absicherung von Infrastruktur-Projekten, wie zum Beispiel Straßen, Brücken, Tunnel usw. Bei dieser Bauwesenversicherung handelt es sich um eine Absicherung von Leistungen, die während eines Bauprojektes erbracht werden. Zusätzlich können auch bestehende Sachwerte über diesen Vertrag versichert werden. Die Laufzeit der CAR-Versicherung richtet sich nach dem Zeitraum des Projektes, sie beginnt bei der Einrichtung der Baustelle und endet nach Übergabe des Projektes. Unter die versicherten Leistungen fallen „Schäden infolge mangelhafter Erstellung der Bauleistung, Brand, Blitzschlag, Explosion, Schäden durch Gewässer und Grundwasser, andere Wittringseinflüsse und noch einiges mehr“ (Ebner 2015, S. 41). Es handelt sich also, wie der Name schon sagt, um eine Allgefahrendekoration, eine „All Risk“ Versicherung. Diverse Ausschlüsse und Selbstbehalte werden vor Vertragsabschluss dokumentiert und auch Zusatzleistungen, wie zum Beispiel die Abdeckung von Maintenance-Leistungen können als Zusatzbausteine miteingeschlossen werden. Die meisten Deckungskonzepte der Versicherer bieten zusätzliche Dienstleistungen zu ihren CAR-Policen an. Hierzu kann die Unterstützung während der Planungsphase inkl. Analysen der wichtigsten Bauunterlagen und Bewertung der Risiken sowie die Unterstützung bei der Kostenverteilung auf die Baube-

teiligen gehören. Die Versicherungssumme für diese spezielle Bauleistungsversicherung setzt sich aus den Herstellungskosten für das gesamte Bauvorhaben (inkl. Eigenleistungen) zusammen. Nicht eingeschlossen werden Grundstücks-, Erschließungs- und Baubebenkosten. Hierzu ein mögliches Schadenbeispiel, welches über eine CAR-Police abgesichert sein kann: Kurz vor Projektzielerreichung, das heißt Fertigstellung des Bauobjektes, kommt es zu einem Einbruch auf der Baustelle. Die Einbrecher stehlen bereits installierte Heizungsanlagen. Durch diesen Vorgang entstehen nicht nur Kosten für die Wiederbeschaffung und Neumontage, sondern auch Kosten für die Reparaturen der Einbruchspuren sowie Kosten für Trocknungen der durch die Demontage ausgetretenen Flüssigkeiten und die entsprechende Verzögerung durch diese Maßnahmen.

Erection All Risk (EAR)

Im Vergleich zu den CAR-Policen umfassen EAR-Policen die Absicherung bei der Errichtung und Installation elektrischer oder mechanischer Anlagen und Maschinen. Diese Versicherungsform wird deswegen auch als Montageversicherung bezeichnet. Der Versicherungsschutz umfasst neben Montageobjekten auch die Montageausrüstung sowie, sofern beantragt, auch fremde Gegenstände, die zur Montage benötigt werden. Versichert sind unter anderem Schäden durch Ungeschicklichkeit, Fahrlässigkeit oder Böswilligkeit, durch Bedienungsfehler, einfache Montagefehler oder auch durch Brand, Blitzschlag, Explosion, durch höhere Gewalt sowie durch Diebstahl (vgl. HDI 2019). Die EAR-Versicherung bietet also Schutz vor finanziellen Verlusten durch plötzlich auftretende, zufällige und unvorhergesehene Ursachen, die zu einem Verlust oder einer Beschädigung der auf der Baustelle versicherten Sachen führen, während sie gelagert, montiert, getestet und in Betrieb genommen werden. Der Versicherungsschutz kann und sollte so gestaltet sein, dass alle beteiligten Haupt- und Subunternehmen mitversichert sind. Im Normalfall besteht bei Montageversicherungen eine Selbstbeteiligung. Der Haftungszeitraum unterliegt bei dieser Versicherungsart gewissen Schwankungen. Denn es kann im Vorfeld nicht genau festgelegt werden, an welchem Tag die Montagetätigkeit letztendlich beginnt. Daraus hängt bei Montageversicherungen als ProjektPolice der Versicherungsbeginn von dem Zeitpunkt ab, an dem die Baustelle eingerichtet wird. Eine Versicherungssumme wird vor Projektbeginn vorläufig bestimmt. Die letztendliche Summe wird dann nach Abschluss des Projektes festgelegt und abgerechnet. Die Versicherungssumme setzt sich aus dem Kontraktprice und den Kosten für Lieferungen und Leistungen des Bestellers zusammen. Die Höhe der Entschädigungsleistung ergibt sich aus dem Wiederbeschaffungswert der beschädigten Sache einschließlich der Aufwendungen für Transport und Montage. Ein mögliches Schadenbeispiel, welches in der Montageversicherung mitversichert ist, wäre folgendes Szenario: Eine Schraube, welche für die Dichtung an einer Wasserkraftwerksturbine verantwortlich ist, wurde mit einem zu hohen Drehmoment angezogen. Dies hat zur Folge, dass im Zuge des Probebetriebes die Dichtung versagt und es zu Schäden an der Einrichtung kommt.

Im Grunde handelt es sich bei beiden Versicherungen um eine vergleichbare Absicherung für sachliche Schäden. Die Absicherung für finanzielle Belastungen aufgrund eines Sachschadens am Liefergegenstand stellt das zentrale Risiko dar, welches abgesichert ist. Der Unterschied liegt einzig in der jeweiligen Art des Bauwerkes.

32.2.1.2 Versicherung der Haftungsrisiken aus einem Projekt

Des Weiteren sollte die Absicherung der aus dem Projekt folgenden Haftungsrisiken, das heißt mögliche Schadenersatzansprüche Dritter, in der Projektversicherung sichergestellt werden. Die Versicherung dieser Risiken kann hier nur kurz dargestellt werden.

Die Haftpflichtversicherung deckt regelmäßig Schadenersatzansprüche Dritter wegen Personen- und Sachschäden einschließlich hieraus resultierender Folgeschäden ab. Ebenfalls gedeckt sollten darüber hinaus auch Schäden durch Umwelteinwirkungen aus den Projektaktivitäten sowie Umweltschäden sein. Neben der Absicherung von Haftpflichtansprüchen aus den vorgenannten Schäden sollte auch in Betracht gezogen werden, in welchem Umfang Ansprüche wegen eines Mangels am Errichtungsobjekt selbst aufgrund fehlerhafter Planungs- und/oder Bauleitung versichert werden sollen.

Bei Projekten handelt es sich im Normalfall um große Baustellen mit unzähligen Gefahrquellen, durch die Außenstehende bzw. die Umwelt im Allgemeinen geschädigt werden können. Der Abschluss einer Haftpflichtversicherung wird meist als Zusatzbaustein zur Projektversicherung angeboten, erfordert aber eine individuelle Ausgestaltung insbesondere dann, wenn Haftungsrisiken im Bereich Umwelt wie auch Planungsobjektschäden einbezogen werden sollen.

32.2.1.3 Vor- und Nachteile der Projektversicherung

Die Absicherung von Projekten in Form einer Projektversicherung hat verschiedene Vor- und Nachteile:

Nachteile

In dem Fall, dass eine Projektversicherung über den Auftragnehmer (in diesem Kapitel nicht behandelt) abgeschlossen wird, sind Schäden durch Service- und Maintenance-Leistungen nicht automatisch mitversichert. Da diese Schäden nach Projektabschluss und somit in der Regel nach Ablauf eines Projektversicherungsvertrages eintreten, müssen für diese Fälle spezielle Vereinbarungen getroffen werden.

Ein weiterer wesentlicher Nachteil bezieht sich auf die zu zahlenden Prämien. Bei Abschluss einer Projektpolice entsteht grundsätzlich ein höherer Prämienaufwand. Dies resultiert aus dem höheren Aufwand der Prüfung, des Abschlusses und der Bearbeitung. Zusätzlich begründet sind die höheren Prämien durch die Tatsache, dass zum Beispiel fünf Mal separat zur Verfügung stehende Versicherungssummen (zum Beispiel jeweils 20.000 Euro) für separate Projekte einen höheren Prämienaufwand auslösen als eine nur einmalig zur Verfügung stehende Versicherungssumme für alle Projekte (zum Beispiel 100.000 Euro).

Vorteile

Allerdings hat der Abschluss einer Projektversicherungspolice auch eine Reihe von Vorteilen: So sind Deckungserweiterungen bei Projektversicherungen einfacher zu integrieren und es gibt weniger Schnittstellen, was zu einer einfacheren Handhabung führt (vgl. Thevis 2018). Projektpolicen profitieren von der individuellen Risikobewertung einzelner Versicherer, da der Risikoappetit und die Risikobewertung einzelner Projekte sich von Versicherer zu Versicherer deutlich unterscheiden können. Somit ergeben sich für jedes neue Projekt neue Möglichkeiten für eine adäquate Absicherung.

Bezüglich des sachlichen Aspekts ergibt sich ein weiterer Vorteil. Durch die exklusive und individuelle Absicherung entsteht zwar ein höherer Aufwand in der Darstellung des Risikos gegenüber dem Versicherer, aber gerade dies trägt auch dazu bei, dass alle besonderen Risiken des konkret abzusichernden Projektes ausreichend berücksichtigt werden können. Diese höhere Risikotransparenz führt dazu, dass Beurteilungsfehler durch eine mögliche Pauschalisierung im Rahmen von Jahresverträgen besser vermieden werden.

Ein weiterer Vorteil besteht mit Blick auf Kostentragung. Denn die Prämie für eine Projektversicherung kann unternehmensintern leichter verursachungsgerecht zugeordnet werden. Und etwaige Höchstgrenzen müssen nicht mit anderen Projekten verrechnet werden, sondern stehen einzlig und allein dem abgesicherten Projekt zur Verfügung.

Auch die Regelung der Selbstbeteiligung spielt in der Projektabsicherung eine wichtige Rolle. Bei der Absicherung über Projektpolicen kann weitergehender und einfacher auf spezielle Forderungen eingegangen werden.

Schließlich ist es von Vorteil, dass bei Abschluss einer Projektversicherung vermieden werden kann, dass die Projektrisiken den Gesamtversicherungsbestand belasten, was bei Einstchluss der Projektrisiken in die bestehenden Versicherungsprogramme der Fall sein kann. Denn während des Projektes müssen oft auch die Leistungen von Sub- oder Nachunternehmen mit abgesichert werden. Bettet der Auftraggeber diese Risiken vollumfänglich in seine bestehenden Jahresverträge mit ein, ist das Risiko hoch, dass er mit projektbezogenen Schäden dann seinen Gesamtversicherungsbestand belastet. Eine separate Projektversicherung verhindert diese Gefahr (vgl. Torbohm).

32.2.2 Schnittstellen zu anderen Versicherungen

Während eines Projektes können bzw. sollten weitere Versicherungen, wie zum Beispiel eine spezielle Betriebsunterbrechungsversicherung zur Absicherung von Ertragsausfällen durch Verzögerungen in der Inbetriebnahme, abgeschlossen werden (vgl. Ebner 2015, S. 41). Beispielhaft kann hier eine Mietausfallsversicherung genannt werden, über die das Risiko nicht realisierter Mieteinnahmen aufgrund einer Verzögerung bei der Projektfertigstellung in Folge eines versicherten Bauleistungsschadens abgesichert werden kann. Vergleichbare Versicherungen werden auch für andere Risikokonstellationen angeboten, wie zum Beispiel „Delay in Start Up“ (DSU) oder „Advance Loss of Profit“ (ALOP).

Der Vollständigkeit halber ist zu hervorzuheben, dass häufig noch zusätzliche Versicherungen für die Absicherung der am Projekt beteiligten Arbeitskräfte abgeschlossen werden müssen, zum Beispiel Krankenversicherungen oder Arbeitsunfähigkeitsversicherungen. Außerdem müssen die Transportmittel und weitere Kfz über eine Kfz-Versicherung abgesichert werden.

32.3 Fazit

In diesem Kapitel ist deutlich herausgearbeitet worden, dass die Verknüpfung zwischen Projektmanagement und Industriever sicherungslösungen für Projekte von großer Bedeutung ist. Die hohe Anzahl möglicher Risiken muss dabei eingehend identifiziert und analysiert sowie hinsichtlich ihrer möglichen Auswirkungen ein- und abgeschätzt werden, da auf dieser Basis erst Entscheidungen zu ihrer Absicherung getroffen werden können. Zentrale Bedeutung kommt den Verflechtungen zwischen dem Management und der Versicherung dieser Risiken zu. Die Klärung der einzelnen Beziehungen, die Ordnung der Haftungsansprüche und die vertraglichen Vereinbarungen darüber, welche Vertragspartei welche Risiken trägt und welche Vertragspartei die Entscheidung zum Abschluss welcher Versicherung trifft, stellen eine komplexe Herausforderung für alle beteiligten Parteien dar.

Sind diese Punkte geklärt, stellt dies eine Grundvoraussetzung für ein adäquates und konkret auf die Projektrisiken zugeschnittenes Versicherungskonzept dar. Als Ergebnis dieses Kapitels kann festgehalten werden, dass der Abschluss über eine separate Projekt policien zwar mit höheren Versicherungskosten einhergehen kann, dem allerdings als Vorteil eine projektspezifische Versicherungslösung gegenübersteht, deren Vorteilhaftigkeit häufig erst bei Eintritt eines Schadenevents offenkundig wird – jedoch zu diesem Zeitpunkt rückwirkend nicht mehr vereinbart werden kann. Die letztendliche Entscheidung darüber, auf welche Weise ein Projekt abgesichert werden soll, ist immer abhängig von der jeweiligen Risikobereitschaft des verantwortlichen Versicherungsnehmers (in diesem Fall des Auftraggebers). Dieser trägt die Entscheidung unter Berücksichtigung aller am Projekt beteiligten Interessenten. Ebenfalls festzuhalten ist, dass bei Projektversicherungen die Schwierigkeit letztendlich nicht in der finalen Absicherung liegt, denn adäquate und variable Deckungskonzepte und Hilfestellungen von Versicherern am Markt gibt es ausreichend. Viel wichtiger ist in diesem Zusammenhang das Management der Projekte. Die beteiligten Personen und Unternehmen, die verschiedenen Konstellationen und Haftungen, Vertragsbeziehungen und alle anderen besprochenen Einflüsse müssen vollständig erfasst und bewertet werden, damit ein Projekt sowohl unter zeitlichen, qualitativen als auch kostentechnischen Aspekten planmäßig und damit gewinnbringend durchgeführt werden kann. Das Verständnis über die Zusammenarbeit zwischen Projektmanagement und Versicherung und die Berücksichtigung der daraus folgenden Erkenntnisse ist dementsprechend ausschlaggebend für den Erfolg des gesamten Projekts.

Literatur

- Brockhaus Enzyklopädie Online. (2020). Risiko, Versiondatum 31.08.2020. Brockhaus. <https://brockhaus.de/ecs/permalink/2509DD23ED3C0C9EB29C722181D51E6D.pdf>. Zugegriffen am 31.08.2020.
- Ebner, G. (2015). *Bauprojekte: Das „Risiko pur“ professionell managen*. Wien: Immobilien Fokus.
- Ensthaler, J., Gesmann-Nuissl, D., & Müller, S. (2012). *Technik Recht – Rechtliche Grundlagen des Technologiemanagements*. Berlin/Heidelberg: Springer.
- HDI. (2019). *Produktblatt: Montageversicherung*. Hannover: HDI Versicherung. www.hdi.de/produkte.
- Hofmann, Dr. T., & Sinemus, Prof. Dr. K. (2013). *Partizipation – Neue Herausforderung für Kommunikation*. Berlin: Helios Media GmbH.
- Höllen, A., et al. (2010). *Tiefe Geothermie*. Berlin: Verband Beratender Ingenieure VBI.
- Meyer, H., & Reher, H. J. (2016). *Projektmanagement*. Wiesbaden: Springer Gabler.
- Nguyen, T. (2007). *Grenzen der Versicherbarkeit von Katastrophenrisiken*. Wiesbaden: Deutscher Universitätsverlag.
- Romeike, F. (2018). *Risikomanagement*. Wiesbaden: Springer Gabler.
- Rudolf-Miklau, Dr. F., & Suda, Dr. J. (2012). *Bauen und Naturgefahren*. Wien: Springer.
- Thevis, H. (2018). Die kombinierte Bauleistungs- und Haftpflichtversicherung für alle Baubeteiligten. *VersicherungsPraxis*, 2018(04), 11–13.
- Torbohm, L. (2018). Projektversicherungen im Maschinen- und Anlagenbau – Besonderheiten, Vorteile und Nachteile. *VersicherungsPraxis*, 2018(04), 3–8.
- Umnuß, Dr. K. (2017). *Corporate Compliance Checklisten*. München: C.H. Beck.

Lutz Torbohm ist Geschäftsführer der SMS Insurance GmbH, einer Tochtergesellschaft der SMS group GmbH, einem international tätigen Unternehmen des Anlagen- und Maschinenbaus. Herr Torbohm startete, nach Abschluss seines Studiums als Diplom Wirtschaftsingieur, seinen beruflichen Werdegang bei der Gerling Allgemeine Versicherungs-AG. Von 2003 bis 2016 war Herr Torbohm bei der AIG Europe S.A., Direktion für Deutschland, bzw. ihren Vorgängergesellschaften im Bereich Haftpflicht tätig.

Svenja Schröder studierte Versicherungswesen mit den Schwerpunkten Risikomanagement, Bilanzierung von Versicherungsunternehmen und Sachversicherungen am Institut für Versicherungswesen der Technischen Hochschule Köln. Im Anschluss absolvierte sie dort auch das Masterstudium Risk & Insurance.



Rating und Solvency II

33

Hüseyin Kaya und Mergime Rrahimi

Zusammenfassung

Sowohl Ratings als auch Solvency II sind aufsichtsrechtlich überwachte Verfahren, mit denen die Solvenz von Versicherungsunternehmen ermittelt wird. Auf diese Weise sollen sowohl Versicherungsnehmer als auch Kapitalgeber vor Fehlentscheidungen geschützt werden. Um dies zu bewerkstelligen, werden die jeweiligen Informationen veröffentlicht. Neben einigen Gemeinsamkeiten weisen die beiden Modelle allerdings auch Unterschiede auf. Während das Rating auf Freiwilligkeit beruht und einen branchen- sowie länderübergreifenden Gesamtüberblick bietet, bezieht sich die Überprüfung der Solvenzquote nur auf die europäische Versicherungsbranche und ist verpflichtend. Darüber hinaus handelt es sich bei der Überprüfung der Solvenzquote lediglich um eine Status-quo-Betrachtung, da sie nur zu bestimmten Stichtagen ermittelt wird. Eine langfristige Aussage über die Finanzkraft der Versicherer kann nur unter Berücksichtigung der Quote nicht getroffen werden. Im Ratingverfahren werden alle Unternehmensebenen herangezogen, so dass eine umfassende Bewertung des gesamten Versicherungsunternehmens erfolgt. Um dies zu gewährleisten, werden neben öffentlich zugänglichen Informationen auch interne Daten verwendet, wie zum Beispiel Wirtschaftsprüfer- und interne Risikoberichte. Im Gegensatz zu Solvency handelt sich bei Ratings um eine prospektive Analyse. Bei der Urteilsfindung berücksichtigen die Ratinganalysten auch, inwieweit die aufsichtsrechtlichen Anforderungen erfüllt werden.

H. Kaya (✉)

ASSEKURATA Assekuranz Rating-Agentur GmbH, Köln, Deutschland

E-Mail: hueseyin.kaya@assekurata.de

M. Rrahimi

TH Köln, Institut für Versicherungswesen, Köln, Deutschland

E-Mail: mergime.rahimi@outlook.de

Im Besonderen beziehen die Agenturen bei der Beurteilung des Risikomanagements die Anforderungen von Solvency II und die Berichte, wie zum Beispiel den ORSA-Prozess und den ORSA-Bericht, ein.

33.1 Einleitung

Zur Einführung in die Thematik lohnt es sich, zunächst einmal die Versicherungstätigkeit näher zu betrachten. Das Produkt der Versicherungsunternehmen ist das Bereitstellen von Versicherungsschutz. Bei Abschluss eines Versicherungsvertrages erfolgt ein Risikotransfer, das heißt, Risiken werden auf die Bilanz des Versicherers übertragen.

Der Begriff „Risiko“ beschreibt das Wagnis, einen negativen Ausgang in Form von Verlust oder Schaden zu erleiden (vgl. Dudenredaktion). Die negativen Abweichungen werden dementsprechend auf das Versicherungsunternehmen übertragen und der Versicherer kommt anstelle des Versicherungsnehmers für die anfallenden Verwaltungs- und Regulierungskosten auf.

Für diesen Risikotransfer zahlt der Versicherungsnehmer eine Prämie. Anders als bei klassischen Produktionswegen erfolgt in der Versicherungsbranche die Produktion erst nach dem Absatz (vgl. Heep-Altiner et al. 2015, S. 1). Infolgedessen ist eine angemessene Kalkulation der Produktionskosten sehr wichtig. Die Produktionskosten eines Versicherers sind die Leistungsbeträge in einem Versicherungsfall. Da jedoch der Eintritt, der Zeitpunkt und das Ausmaß des Versicherungsfalls ungewiss sind, müssen die Versicherer ausreichend Kapital zur Verfügung haben, um ihren Verpflichtungen jederzeit nachkommen zu können. Das Kapital setzt sich aus den Prämieneinnahmen und den unterlegten Eigenmitteln zusammen. Wird dieses vollkommen verbraucht, so tritt ein Ruin ein. Ein Risiko des Versicherungsunternehmens besteht darin, dass Prämieneinnahmen im Verhältnis zu den anfallenden Versicherungsleistungen zu gering kalkuliert sind. Dieses Risiko wird als versicherungstechnisches Risiko bezeichnet (vgl. Rohlfs 2018, S. 171 ff.).

Für einen reibungslosen Geschäftsablauf im Versicherungsunternehmen müssen die vom Versicherungsunternehmen eingegangen Risiken ausreichend abgedeckt werden. Dafür stellt der Versicherer nicht nur die Prämieneinnahmen sicher, sondern er muss ausreichend „mit Eigenmitteln, also freiem, unbelastetem Vermögen“ (BaFin 2016a) ausgestattet sein (Solvabilität). Die Bestimmung und Bewertung der Solvabilität kann anhand diverser externer und interner Modelle durchgeführt werden, wie zum Beispiel im Solvency II und im Ratingmodell (vgl. Heep-Altiner et al. 2014, S. 27).

Solvency II gehört zu sogenannten Solvenz-Modellen und ist EU-weit am 01.01.2016 in Kraft getreten (vgl. BaFin 2016b). Solvenz-Modelle werden nicht nur in der EU, sondern weltweit angewandt, wie zum Beispiel in der Schweiz in Form des Schweizer Solvenz Tests oder in den Vereinigten Staaten in Form der US-amerikanischen RBC Standards (vgl. Heep-Altiner et al. 2014, S. 29).

Zur Regulierung der Eigenmittel gibt Solvency II zwei Kapitalanforderungen vor: die Solvenzkapitalanforderung bzw. Solvabilitätsanforderung (SCR) und die Mindestkapi-

talanforderung (MCR). Diese Anforderungen stellen sicher, dass der Versicherer genügend verfügbares Eigenkapital besitzt. Zur Berechnung des Solvenzkapitals können sich die Versicherer zwischen einer vorgegebenen Standardformel und einem unternehmenseigenen internen Modell entscheiden. Die Standardformel wird den externen Modellen zur Bestimmung des Kapitalbedarfs zugeordnet.

Ein weiteres externes Modell ist das Ratingmodell, bei dem die Bonität eines Ratingobjektes in Form eines Ratings eingestuft wird. Das Rating wird gemäß der EU-Ratingverordnung definiert als „ein Bonitätsurteil in Bezug auf ein Unternehmen, einen Schuldtitel oder eine finanzielle Verbindlichkeit, eine Schuldverschreibung, eine Vorzugsaktie oder ein anderes Finanzinstrument, das anhand eines festgelegten und definierten Einstufungsverfahrens für Ratingkategorien abgegeben wird“ (Verordnung 1060/2009, Art. 3 Abs. 1a).

Der Ratingprozess erfordert eine Zusammenarbeit zwischen der Ratingagentur und dem zu ratenden Unternehmen. Im Gegensatz zu Solvency II ist ein Rating nicht verpflichtend für Versicherungsunternehmen.

In der vorliegenden Arbeit werden die zwei Systeme Solvency II und das Ratingmodell analysiert. Die Leitfragen dabei sind, wie diese Systeme zueinander stehen und ob Solvency II, genauer gesagt die Solvenzquote, das Rating vollkommen ersetzt hat. Dazu werden zu Beginn beide Modelle erläutert und deren Verfahren und Ziele in der Versicherungsbranche dargestellt. Die Stärken und Schwächen sowie Gemeinsamkeiten und Unterschiede werden dargelegt und auf deren Basis Stellung zu den Leitfragen genommen.

33.2 Rating

33.2.1 Definition

Ratings dienen zur Klassifizierung der Bonität und Kreditwürdigkeit eines Ratingobjektes und orientieren sich bei der Beurteilung und Einstufung an einer sogenannten Ratingskala. Ratingobjekte können Unternehmen, Länder und Wertpapiere sein. Ratings dienen dazu, Informationsasymmetrien zu verringern, und erfüllen den Zweck, die Anlage- und Finanzentscheidung der Stakeholder (Eigenkapitalgeber) zu unterstützen (vgl. Rohlf 2018, S. 139 ff.).

33.2.1.1 Ratingagentur

Ratings werden durch sogenannte Ratingagenturen ermittelt. Die Agenturen vergeben durch Informationserhebung und -bewertung ein Urteil über die Bonität und die Kreditwürdigkeit des Ratingobjektes in Form einer Note (vgl. Rohlf 2018, S. 140). Dabei ist die Vergabe dieser Urteile ausschließlich sogenannten „External Credit Assessment Institutionen“ (ECAI) vorbehalten. ECAI-Agenturen sind nach Art. 4 I Nr. 98 Capital Requirements Regulation (CRR) anerkannte Ratingagenturen (vgl. Blaß 2018). Erst mit der Genehmigung durch die Europäische Union dürfen die Agenturen somit ihre Tätigkeit

aufnehmen. Dabei unterliegen sie der europäischen Wertpapieraufsicht ESMA (European Securities und Markets Authority, dt. Europäische Wertpapier- und Marktaufsichtsbehörde) (vgl. Goller 2013). Zu den bekanntesten Agenturen zählen zum Beispiel Standard & Poor's (S&P), Moody's, Fitch, A.M. Best und die ASSEKURATA als spezialisierte deutsche Ratingagentur in der Versicherungsbranche.

33.2.1.2 Interaktive und Public Information Ratings

Bei veröffentlichten Ratings wird zwischen interaktiven Ratings und Public Information Ratings unterschieden.

Für die Ermittlung von Public Information Ratings, kurz PI-Ratings, greifen die Ersteller nur auf öffentlich zugängliche Informationen zurück, so dass sie zumeist ohne Auftragserteilung erstellt werden (vgl. Versicherungsmagazin o. J.). Dies schmälert allerdings die Aussagekraft der Urteile.

Im Gegensatz zu Public Information Ratings basieren interaktive Ratings auf einer Zusammenarbeit zwischen Ratingagentur und Ratingobjekt, in der Versicherungsbranche dem gerateten Versicherungsunternehmen. In interaktive Ratings fließen somit neben externen auch interne, also öffentlich nicht zugängliche, Daten ein. Hierbei handelt es sich zum Beispiel um Wirtschaftsprüfberichte und interne Risikoberichte.

Anders als bei den PI-Rating-Urteilen zahlen die zu ratenden Unternehmen für die Durchführung eines interaktiven Ratings ein Honorar. Außerdem werden die qualitativen und quantitativen Stärken sowie Schwächen beim interaktiven Rating genauer analysiert und umfangreicher betrachtet. Aus diesem Grund ist eine gute Zusammenarbeit zwischen der Ratingagentur und dem Ratingobjekt Voraussetzung.

In der deutschen Versicherungsbranche verfügte im Jahre 2019 Moody's mit über 30 Prozent über den größten Marktanteil an interaktiven Ratings, gefolgt von der Assekurata mit 25 Prozent, Fitch mit 23 Prozent und Moody's und A. M. Best mit jeweils elf Prozent (vgl. Abb. 33.1).

33.2.2 Unterschied zwischen Unternehmens- und Bonitätsrating

Im Ratingprozess unterscheidet Assekurata zwischen dem Unternehmens- und dem Bonitätsrating. Die Differenzierung der beiden Ratings liegt hauptsächlich in der Fristigkeit. Während Unternehmensratings kurzfristig angelegt sind, ist das Bonitätsrating eine langfristige Bewertung der Finanzstärke des Unternehmens.

33.2.2.1 Unternehmensrating

Das Unternehmensrating betrachtet und bewertet das Unternehmen ganzheitlich und berücksichtigt dabei die Kundensicht. Dafür werden auch Kundenzufriedenheits- und Kundenbindungsindizes durch Kundenbefragungen ermittelt.

Die Analyse und Bewertung des Unternehmens umfasst vier bzw. fünf Teilqualitäten. Anhand von qualitativen und quantitativen Kennzahlen werden diese einzeln bewertet:

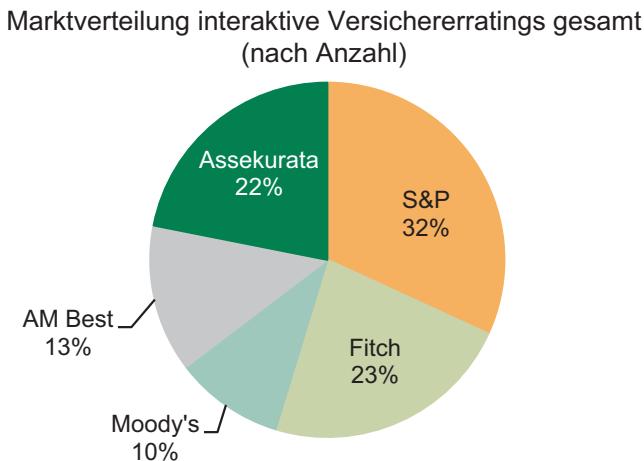


Abb. 33.1 Marktanteile Versicherungsratingagenturen in Deutschland. (Quelle: eigene Darstellung, eigene Erhebung, Stand: August 2019)

- Sicherheit,
- Erfolg,
- Kundenorientierung (inklusive Kundenbefragung),
- Wachstum/Attraktivität im Markt,
- Beitragsstabilität (nur in der Krankenversicherung).

Die verschiedenen Perspektiven werden im Einzelnen detailliert betrachtet und am Ende mithilfe von Checklisten zusammengeführt.

33.2.2.2 Bonitätsrating

Das Bonitätsrating beurteilt explizit die Bonität und Finanzlage des Ratingobjektes. Es wird eine Aussage darüber getroffen, wie liquide das betrachtete Unternehmen ist. Die Bestimmung der Bonitätseinstufung erfolgt anhand von Kennzahlen, Steuerungsfaktoren und Rahmenfaktoren. Die Kennzahlen werden in die Kategorien Sicherheit, Wachstum und Erfolg unterteilt. Diese Kategorisierung ist zum Großteil übereinstimmend mit der Ratingmethodik des Unternehmensratings (vgl. Abb. 33.2).

Die Sicherheitskennzahlen für Schaden- und Unfallversicherer sind zum Beispiel:

- Eigenkapitalquote = Eigenkapital in Prozent der gebuchten Prämie für eigene Rechnung,
- versicherungstechnische Spezialkapitalquote = Versicherungstechnisches Spezialkapital (Schwankungsrückstellung + Drohverlustrückstellung) in Prozent der gebuchten Prämie für eigene Rechnung,
- SCR-Quote = Verhältnis von den Eigenmitteln zur Solvenzkapitalanforderung,
- Schadenreservequote brutto = Schadenrückstellung brutto in Prozent der gebuchten Bruttoprämie.

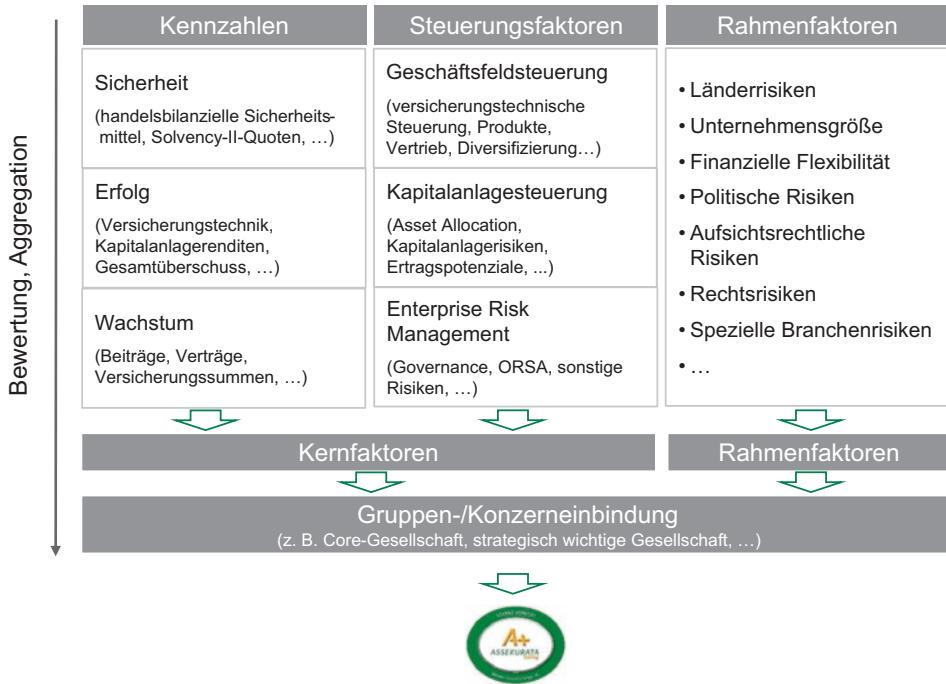


Abb. 33.2 Aufbau des Assekurata-Bonitätsratings. (Quelle: eigene Darstellung)

Zu den Erfolgskennzahlen von Schaden- und Unfallversicherern gehören zum Beispiel:

- Schadenquote brutto = Schadenaufwand brutto in Prozent der verdienten Bruttoprämien,
- Verwaltungskostenquote brutto = Verwaltungskosten brutto in Prozent der verdienten Bruttoprämien,
- Abschlusskostenquote brutto = Abschlusskosten brutto in Prozent der verdienten Bruttoprämie,
- Combined Ratio brutto = Schadenaufwand brutto + Verwaltungskosten brutto + Abschlusskosten brutto in Prozent der verdienten Bruttoprämien,
- Erfolgskennzahlen der Kapitalanlage, wie zum Beispiel die Nettoverzinsung.

Die Wachstumskennzahlen können sein:

- Zuwachsrate gebuchter Bruttoprämien,
- Zuwachsrate Vertragsstückzahlen.

In einer Kennzahlanalyse werden diese Kennzahlen ökonomisch eingeordnet. Auch die aufsichtsrechtliche Solvabilität nach Solvency II findet im Rahmen der Analyse der Sicherheitskennzahlen ihre Berücksichtigung.

Die Geschäftsfeldsteuerung, die Kapitalanlagesteuerung und das Enterprise Risk Management bilden die Steuerungsfaktoren und ergänzen die Kennzahlanalyse um eine umfassende qualitative Prüfung. Dadurch formen die Steuerungsfaktoren zusammen mit den ökonomischen Geschäftskennzahlen die Kernfaktoren, auf deren Basis das Gesamtrating erstellt wird. Berücksichtigt werden zudem die Rahmenfaktoren zum Geschäfts- und Unternehmensumfeld. Diese spiegeln insbesondere Risiken aus dem Markt, der Branche, der Unternehmensgröße, der Unternehmensorgane, der IT-Infrastruktur, der Geschäftsregion, der Wettbewerbspositionierung sowie politische und rechtliche Risiken in ihrer Wirkung auf das Unternehmen wider.

Durch die Zusammensetzung und Analyse der Kern- und Rahmenfaktoren erfolgt eine ausführliche Prüfung der Chancen und Risiken des gerateten Unternehmens. Dies gewährt eine umfangreiche Betrachtung auf die Bonitätslage des Versicherungsunternehmens, auf deren Basis ein Rating zu vergeben ist.

33.2.3 Durchführung: Ratingprozess

Im folgenden Abschnitt wird der Assekurata-Ratingprozess erläutert. Die Durchführung der Ratingbestimmung kann je nach Ratingagentur unterschiedlich verlaufen.

Die Ratingprozesse von Bonitäts- und Unternehmensratings sind nahezu identisch. Bei eventuellen Unterscheidungen werden diese in den einzelnen Phasen genannt und erläutert.

33.2.3.1 Auftragserteilung

Im ersten Schritt wird ein Vertrag zwischen dem Versicherer und der Ratingagentur geschlossen. Dieser dient unter anderem zur Sicherheit der Informations- und Datenbewahrung, da das geratete Unternehmen im Verlauf des Ratings diverse interne und sensible Informationen offenzulegen hat. Ob das Ergebnis im Endeffekt an die Öffentlichkeit weitergegeben wird oder nicht, entscheidet das Ratingobjekt. Dieses Wahlrecht wird im Vertrag festgehalten und soll die Zusammenarbeit fördern. Das Unternehmen und die Führungskräfte sollen ehrlich und offen auf sensible Fragen antworten können, ohne negative Folgen für das Unternehmen befürchten zu müssen.

33.2.3.2 Datenerhebung und Datenbereitstellung

Im nächsten Schritt werden mithilfe von Listen Daten erhoben. Die Liste umfasst die Informationsanforderungen, Daten und Unterlagen, die eine umfassende Übersicht und einen Einblick für das Rating ermöglichen. Umfang und Inhalt der Liste ist dabei von der Art des Ratings abhängig und variiert je nachdem, ob es sich um ein Erstrating oder ein Folgerating handelt, also bereits in der Vergangenheit ein Assekurata-Rating durchgeführt wurde. Assekurata deckt mit der Liste mehrere Unternehmensbereiche ab, um sich für die

Interviews mit dem Management (Managementinterviews) vorzubereiten. Betrachtungsgegenstand sind dabei die folgenden Unternehmensbereiche:

- Unternehmensstruktur/Strategie,
- Rechnungswesen/Controlling,
- Vertrieb/Produkte,
- Versicherungstechnik,
- Kapitalanlagen,
- Risikomanagement,
- Kundenorientierung.

Für das Unternehmensrating findet in dieser Phase zusätzlich die Datenselektion und Durchführung der Kundenbefragung statt. Dabei erhält die Assekurata Unterstützung von einem Feldforschungsinstitut.

In den Managementinterviews befragt das Assekurata-Ratingteam die Führungskräfte des Unternehmens. Infolgedessen werden Einblicke in die Unternehmenskultur gewährt, die in der Ratingvergabe berücksichtigt werden. Unter verschiedenen Aspekten wird in den Gesprächen die Qualität des Unternehmens betrachtet. Dabei geben die Manager unter anderem Auskunft zu folgenden Themen:

- Marktentwicklung,
- Unternehmensstrategie,
- Risikomanagement,
- Personalentwicklung,
- Rückversicherungspolitik,
- Produktgestaltung,
- Kapitalanlagestrategie,
- Vertriebswegestruktur,
- Kalkulationsgrundlage,
- Risikoannahmepolitik,
- Beitragsentwicklung,
- Kundenservice.

33.2.3.3 Analyse und Bewertung

In der nächsten Phase werden die gesammelten Informationen analysiert und bewertet. Dafür werden Daten und Ergebnisse der vorherigen Schritte abgeglichen und anhand qualitativer und quantitativer Kriterien analysiert.

Für das Unternehmensrating werden die vier bzw. fünf Teilqualitäten „Sicherheit“, „Erfolg“, „Beitragsstabilität“ (nur in der Krankenversicherung), „Kundenorientierung“ und „Wachstum/Attraktivität im Markt“ mithilfe von Zeitreihen und Benchmarking analysiert und bewertet. Jede Dimension hat dabei ihre eigenen Kennzahlen, deren Ergebnisse in den nächsten Schritten die endgültige Beurteilung bilden. Währenddessen ist eine fortlaufende

Dokumentation notwendig, die in einem sogenannten Ratingbericht festzuhalten ist. Auf dieser Basis diskutiert das Ratingteam den Notationsvorschlag für das Ratingkomitee. Hierbei trägt jedes Teammitglied die Verantwortung für das Rating und die Qualität des Ratingberichts mit.

33.2.3.4 Beschlussfassung im Ratingkomitee

Das Ratingkomitee setzt sich aus dem jeweiligen leitenden Ratinganalysten, einem Bereichsleiter Analyse und Bewertung und mindestens zwei externen Experten zusammen. Damit handelt es sich beim Rating der Assekurata um eine Experteneinschätzung. Für die externen Ratingkomitee-Mitglieder gelten die gleichen Anforderungen an die Unabhängigkeit wie für interne Ratinganalysten: Ein Mitglied des Ratingkomitees wird aus dem Rating ausgeschlossen, sofern seine Unabhängigkeit angezweifelt werden könnte. Dies wäre insbesondere dann der Fall, wenn das Mitglied Funktionen, zum Beispiel in einem Aufsichtsgremium, bei dem zu ratenden Versicherer innehat. In einem solchen Fall erhält das Ratingkomitee-Mitglied weder den Ratingvorschlag noch kann es an der Sitzung teilnehmen. Die Unabhängigkeit der Assekurata ist zudem in ihrer Satzung festgeschrieben und kann auch von der Gesellschafterversammlung nicht geändert werden.

33.2.3.5 Ratingskala

Die Ratingvergabe erfolgt anhand der Ratingskala. Für das Bonitäts- und Unternehmensrating werden dafür zwei verschiedene Skalen angewandt. Die Skala für Bonitätsratings entspricht internationalem Standard, während es die Skala des Unternehmensratings in dieser Form nur bei Assekurata gibt. Darüber hinaus enthält die Bonitätsratingsskala im Gegensatz zur Skala des Unternehmensratings eine größere Differenzierung innerhalb der Ratingklassen durch Anwendungen von Notches (vgl. Rohlfs 2018, S. 365). Plus- und Minuszeichen ermöglichen auf diese Weise eine präzise Bonitätseinstufung.

Eine genaue Gegenüberstellung ist in der Durchführungsverordnung 2016/1800 zu finden (vgl. DVO (EU) 2016/1800, Anhang S. 4). Darin sind alle Ratingagenturen der EU mit ihren Ratings und den dazugehörigen Ratingskalen aufgeführt (vgl. Tab. 33.1).

Im Bonitätsrating vergeben die Analysten zusätzlich einen Ratingausblick. Dieser ist unterteilt in die Kategorien negativ, stabil und positiv. Ein positiver oder negativer Ra-

Tab. 33.1 In Anlehnung an „Gegenüberstellung der Assekurata-Skalen“ (DVO (EU) 2016/1800, Anhang S. 4)

Stufe	Skala für das Bonitätsrating (langfristig)	Skala für das Unternehmensrating (kurzfristig)
0	AAA	
1	AA	A++
2	A	A
3	BBB	
4	BB	B, C, D
5	B	
6	CCC, CC/C, D	

tingausblick wird dabei in der Regel zwischen sechs Monaten und zwei Jahren aufrechterhalten. Danach erfolgt entweder eine Anpassung des Ratings oder des Ratingausblicks. Somit impliziert der positive oder negative Ratingausblick nicht zwingend eine Ratingveränderung.

33.2.3.6 Bekanntgabe des Ratings

Über das endgültige Rating wird der Vorstand des gerateten Unternehmens am Tag der Entscheidung schriftlich (und in der Regel zusätzlich telefonisch) informiert. Dies liegt im Verantwortungsbereich des leitenden Ratinganalysten. Hier hat der Vorstand die Möglichkeit, sich für oder gegen eine Veröffentlichung des Ratings zu entscheiden. Unabhängig von der Entscheidung erhält das geratene Unternehmen einen Bericht mit allen gewonnenen Erkenntnissen und Ergebnissen, evtl. erfolgt dies auch in Form einer Abschlusspräsentation.

Wird der Veröffentlichung schriftlich zugestimmt, erfolgt die öffentliche Bekanntgabe innerhalb von fünf Werktagen nach Beschlussfassung durch das Ratingkomitee. Das Unternehmensrating hat im Vergleich zum Bonitätsrating nur eine Gültigkeit von einem Jahr. Das Bonitätsrating ist hingegen langfristig ausgelegt. Beide Ratings werden einem Monitoring unterzogen. Die laufende Überprüfung stellt sicher, dass die Validität des Ratings im Zeitverlauf gewährleistet ist.

33.2.3.7 Ratingpublikation

Für die Bekanntgabe des Ratings gibt es verschiedene Möglichkeiten. Die Optionen sind:

- **Pressemitteilung:** Die Assekurata informiert die Öffentlichkeit durch eine Pressemitteilung.
- **Ratingbericht:** Die Analysten fassen das Rating in einem öffentlich zugänglichen Bericht zusammen. Diesen stellt die Assekurata auf ihrer Website zum kostenlosen Lesen und Herunterladen zur Verfügung.
- **Gütesiegel:** Gütesiegel erfüllen einen hohen Standard. Geratete Unternehmen validieren ihre Qualität mithilfe der Gütesiegel am Markt.
- **Datenspeicher der Europäischen Aufsichtsbehörde ESMA:** Die europäische Wertpapierbehörde ESMA fordert von jeder Ratingagentur, das veröffentlichte Rating an einen zentralen Datenspeicher der Behörde zu melden.
- **Ratingplattform:** Als Mitglied der European Association of Credit Rating Agencies (EACRA) hat sich Assekurata dazu bereit erklärt, ihre Ratings auf der von EACRA unterstützten globalen Ratingplattform zu veröffentlichen.

33.2.3.8 Anpassung und Aberkennung von Ratings

Treten im Gültigkeitszeitraum außerordentliche Ereignisse oder Entwicklungen auf, die sich auf die Bewertung des Unternehmens auswirken, kann Assekurata das Rating jederzeit anpassen. Sofern es aus Sicht von Assekurata einer Ratinganpassung bedarf, informiert Assekurata das betroffene Unternehmen. Die Information der Öffentlichkeit ge-

schieht durch die Aufnahme der betroffenen Ratings auf die Watchlist und eine entsprechende Presseerklärung. Der Ratingbericht wird dabei nicht angepasst. Für die Überprüfung fordert Assekurata vom Unternehmen detaillierte Informationen, die das Rating betreffen. Ratings auf der Watchlist müssen nicht zwangsläufig zu einer Veränderung der Rating-Notation führen. Das Ratingkomitee von Assekurata entscheidet darüber, ob der Ratingausblick oder das Rating gegebenenfalls angepasst werden müssen (Upgrading oder Downgrading). Ist dies der Fall, wird der Ratingbericht entsprechend angepasst.

Ein veröffentlichtes Rating wird dann aberkannt, wenn durch besondere Entwicklungen (zum Beispiel durch Fusion, Bestandsübertragungen o. ä.) die Grundlagen für das veröffentlichte Rating entzogen sind. In diesem Fall unterrichtet Assekurata die Öffentlichkeit in Form einer Pressemitteilung. Das Unternehmen hat das Recht, unmittelbar im Anschluss an die Aberkennung ein neues Rating in Auftrag zu geben. Gleichzeitig kann das Unternehmen die Öffentlichkeit über die laufende Überarbeitung des aberkannten Ratings in Kenntnis setzen.

33.3 Solvency II

33.3.1 Definition

Solvency II ist eine EU-Richtlinie (vgl. Richtlinie 2009/138/EG), deren Regeln seit dem 01.01.2016 gelten. Das Solvabilitätssystem harmonisierte die bis dahin geltende eher re-

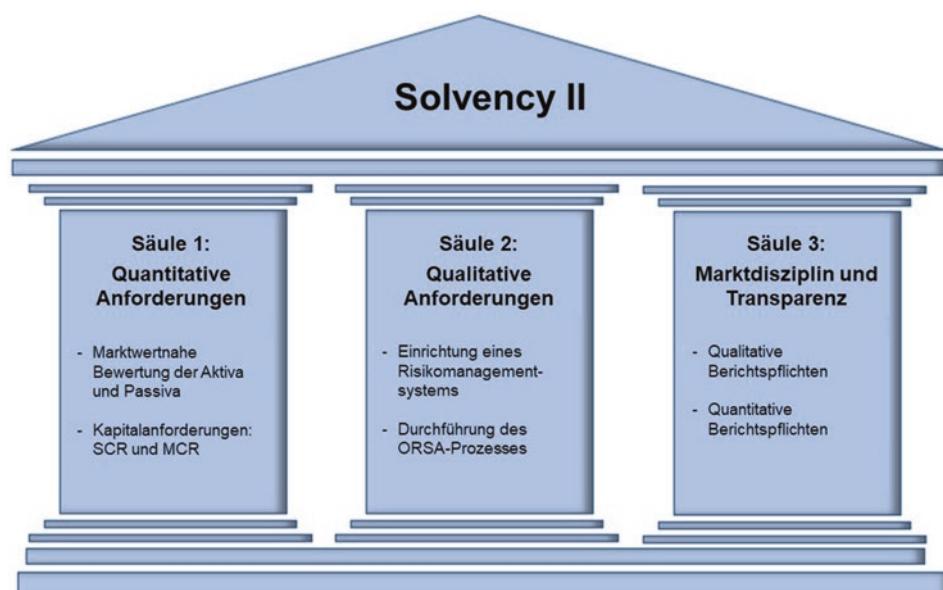


Abb. 33.3 Drei-Säulen-Modell von Solvency II. (Quelle: eigene Darstellung in Anlehnung an Rohlfs 2018, S. 88)

gelorientierte Aufsicht in der europäischen Union. Solvency II ist prinzipienorientiert, die konkrete Ausgestaltung soll unter Berücksichtigung des individuellen Geschäftsmodells und der Risikoexponierung von den Versicherungsunternehmen und der Aufsicht vorgenommen werden (Proportionalitätsprinzip) (vgl. Gründl und Kraft 2019, S. 1). Es dient zum Schutz des Versicherungsnehmers durch (strenge) Anforderungen an die Eigenkapitalausstattung und an das Risikomanagement. Zudem soll auf diese Weise der europäische Binnenmarkt gestärkt werden (vgl. BaFin 2016b).

Solvency II ist an die Eigenkapitalvorschriften der Bankenwirtschaft „Basel II“ angelehnt, weshalb sich die aufsichtsrechtlichen Anforderungen an die Versicherungsunternehmen in einem Drei-Säulen-Modell darstellen lassen (vgl. Abb. 33.3). Das Modell umfasst sowohl quantitative und qualitative Anforderungen als auch Vorschriften zur Förderung der Marktdisziplin und Transparenz.

33.3.2 Säule 1: Quantitative Anforderungen

In der ersten Säule werden die quantitativen Anforderungen zur Solvabilität geregelt. Dabei handelt es sich um Vorschriften, die der Bewertung der Aktiva und Passiva sowie der Bestimmung und Klassifizierung der Eigenmittel dienen.

33.3.2.1 Bewertung der Aktiva und Passiva

Solvency II sieht eine marktwertnahe Bewertung der Vermögensgegenstände und Verpflichtungen vor. Demnach werden Bilanzposten mit dem Wert bewertet, zu dem diese zwischen „sachverständigen vertragswilligen und voneinander unabhängigen Geschäftspartnern getauscht werden könnten“ (vgl. § 74 Abs. 2 VAG). Wird ein Vermögensgegenstand oder eine Verpflichtung in einem liquiden Markt gehandelt, muss der Bilanzposten

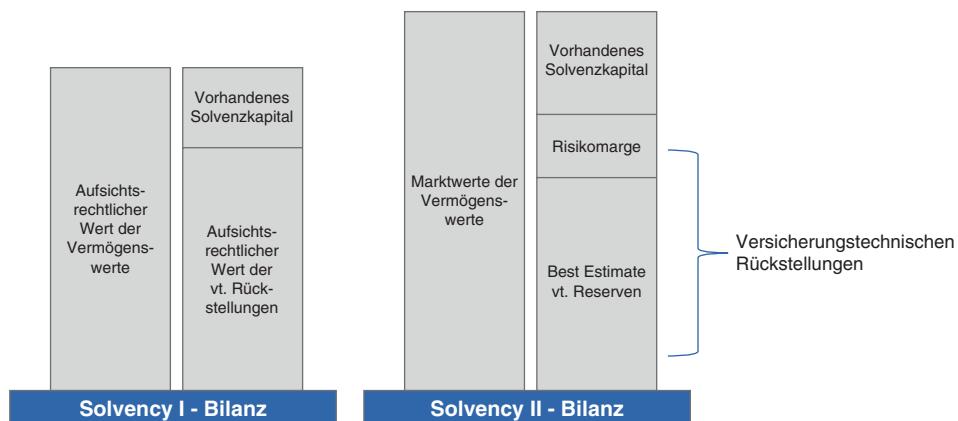


Abb. 33.4 HGB-Bilanz vs. Marktwertbilanz. (Quelle: eigene Darstellung in Anlehnung an ASSE-KURATA Assekuranz-Rating Agentur GmbH o. J.)

gemäß dem Mark-to-Market-Ansatz zu dem beobachtbaren Marktpreis (Marktwert) bilanziert werden (vgl. § 76 Abs. 2 VAG). Ist ein beobachtbarer Marktpreis nicht vorhanden, erfolgt die Bilanzierung nach dem Mark-to-Model-Ansatz, in dem ein solcher Marktwert modellbasiert ermittelt wird. Die modellbasierte Ermittlung gilt insbesondere für die versicherungstechnischen Rückstellungen.

Unter dem Vorgänger Solvency I erfolgte insofern die Bewertung der Aktiva und Passiva nach dem Vorsichtsprinzip, als dass die Aktivposten unterbewertet und die Passivposten überbewertet wurden. Dieses Prinzip orientierte sich am HGB. Damit sollte eine hohe Sicherheit in Form von stillen Reserven und Lasten in der Bilanz gewährleistet werden, wobei jedoch die Solvabilität der Versicherer nicht realitätsnah abgebildet wurde (vgl. Heep-Altiner et al. 2015, S. 202). Aus diesem Grund wurde mit der Reform der Solvabilitätsregeln einheitlich auf die Mark-to-Market-Bewertung umgestellt (vgl. Abb. 33.4).

Die Posten der Aktivseite der Bilanz können in der Regel gemäß dem Mark-to-Market-Ansatz zu beobachtbaren Marktwerten angesetzt werden. Die versicherungstechnischen Rückstellungen werden nach dem Mark-to-Model-Ansatz ermittelt und ihr Wert entspricht der Summe aus dem besten Schätzwert und der Risikomarge (vgl. § 76 VAG). Während der beste Schätzwert dem wahrscheinlichkeitsgewichteten Durchschnitt künftiger Zahlungsströme unter Berücksichtigung des Zeitwerts des Geldes (erwarteter Barwert künftiger Zahlungsströme) und unter Verwendung der maßgeblichen risikofreien Zinskurve entspricht (vgl. § 77 Abs. 1 VAG), stellt die Risikomarge sicher, dass der Wert der versicherungstechnischen Rückstellungen dem Betrag entspricht, den die Versicherungsunternehmen fordern würden, um die Versicherungsverpflichtungen übernehmen und erfüllen zu können (vgl. § 78 VAG).

Damit Versicherungsunternehmen die von ihnen eingegangenen Risiken mit hoher Wahrscheinlichkeit finanziell absichern können, müssen sie mit adäquaten Eigenmitteln ausgestattet sein. Hierbei wird zwischen Basiseigenmitteln und ergänzenden Eigenmitteln unterschieden (vgl. § 89 VAG).

33.3.2.2 Kapitalanforderungen

Die Kapitalanforderungen werden unterteilt in Solvenzkapitalanforderung (Solvency Capital Requirement), kurz SCR, und Mindestkapitalanforderung (Minimum Capital Requirement), kurz MCR.

Die Solvabilitätskapitalanforderung spiegelt alle quantifizierbaren Risiken wider, denen das Versicherungsunternehmen ausgesetzt ist. Diese werden risikobasiert durch den Value-at-Risk-Ansatz ermittelt. Der Value-at-Risk stellt sicher, dass die Höhe der vorhandenen Eigenmittel ausreicht, um unerwartete Verluste abzudecken. Definiert wird der Value-at-Risk als der „Wert, der in einem vorgegebenen Zeitraum und mit einer bestimmten Wahrscheinlichkeit (Konfidenzniveau) nicht über- bzw. unterschritten werden darf.“ (Rohlf 2018, S. 377). Der Zeitraum beträgt ein Jahr und das Konfidenzniveau 99,5 Prozent (vgl. § 97 VAG).

Die Solvabilitätskapitalanforderung kann mithilfe einer Standardformel oder eines internen Modells ermittelt werden (vgl. § 96 VAG). Die Standardformel umfasst gemäß § 99

VAG die Basissolvabilitätskapitalanforderung, die Kapitalanforderung für das operationelle Risiko und die Anpassung für die Verlustausgleichsfähigkeit der versicherungstechnischen Rückstellungen und latenten Steuern, auch Adjustierung genannt.

Das MCR stellt eine Kapitaluntergrenze dar, die bei dauerhafter Unterschreitung bis zum Entzug der Erlaubnis des Geschäftsbetriebs führen kann (vgl. Gründl und Kraft 2019, S. 54). Wird das MCR unterschritten oder droht dieser Fall innerhalb der nächsten drei Monate einzutreten, muss der Versicherer die Aufsichtsbehörde unverzüglich unterrichten und einen Finanzierungsplan vorlegen, der eine Erhöhung der Eigenmittel und/oder Senkung des Risikoprofils darlegen muss.

Die Solvenzquote, auch SCR-Quote genannt, ist das Verhältnis der Eigenmittel (Ist-Kapital) zur Solvabilitätskapitalanforderung (Soll-Kapital). Das Ergebnis muss mindestens 100 Prozent sein, erst dann ist eine ausreichende Kapitalausstattung gemäß des SCR gegeben (vgl. Heep-Altiner et al. 2014, S. 30). Zur Bestimmung der Solvenzquote wird das SCR durch die Standardformel oder ein internes Modell berechnet.

Die Standardformel umfasst gemäß § 99 VAG die Basissolvabilitätskapitalanforderung, die Kapitalanforderung für das operationelle Risiko und die Anpassung für die Verlustausgleichsfähigkeit der versicherungstechnischen Rückstellungen und latenten Steuern, auch Adjustierung genannt. Ziel der Standardformel ist eine vereinfachte und schematische Abbildung der Risikosituation der Versicherungsunternehmen. Ein internes Modell kann das unternehmensindividuelle Risikoexposure, welchem die Versicherer ausgesetzt sind, detaillierter messen und abbilden als die Standardformel (vgl. Gründl und Kraft 2019, S. 55).

Die Standardformel folgt bei der Berechnung des SCR einem modularen Ansatz. In einem Bottom-up-Ansatz werden zunächst Teil-SCR in Untermodulen ermittelt und danach werden diese unter Berücksichtigung von Diversifikationseffekten zu einem Gesamt-SCR aggregiert (Abb. 33.5).

Das Gesamt-SCR berechnet sich in der Standardformel durch die Addition des BSCR (Basisolvenzkapital), der Adjustierung/Anpassung und des operationellen Risikos.

$$\text{SCR} = \text{Basis SCR} + \text{SCR}^{\text{op.Risiko}} + \text{Adjustierung} \quad (33.1)$$

Das BSCR ist die Aggregation aller Einzel-SCR, das heißt, man bestimmt erst die Einzel-SCR des Marktrisikos, Versicherungsrisikos (jeweils für Leben, Nicht-Leben und Kranken), Ausfallrisikos und des immateriellen Vermögenswertes und aggregiert diese nach dem Kovarianzprinzip. Hierbei wird die Korrelation zwischen den Einzel-SCR beachtet. Dadurch ist das Gesamt-SCR aufgrund der Diversifikationseffekte kleiner als die Summe aller Einzel-SCR.

$$\text{Basis SCR} = \sqrt{\left(\sum_{i,j} \text{Corr}_{i,j} x\text{SCR}_i x\text{SCR}_j \right)} \quad (33.2)$$

$\text{Corr}_{i,j}$

Angaben in Zeile i und Spalte j der Korrelationsmatrix

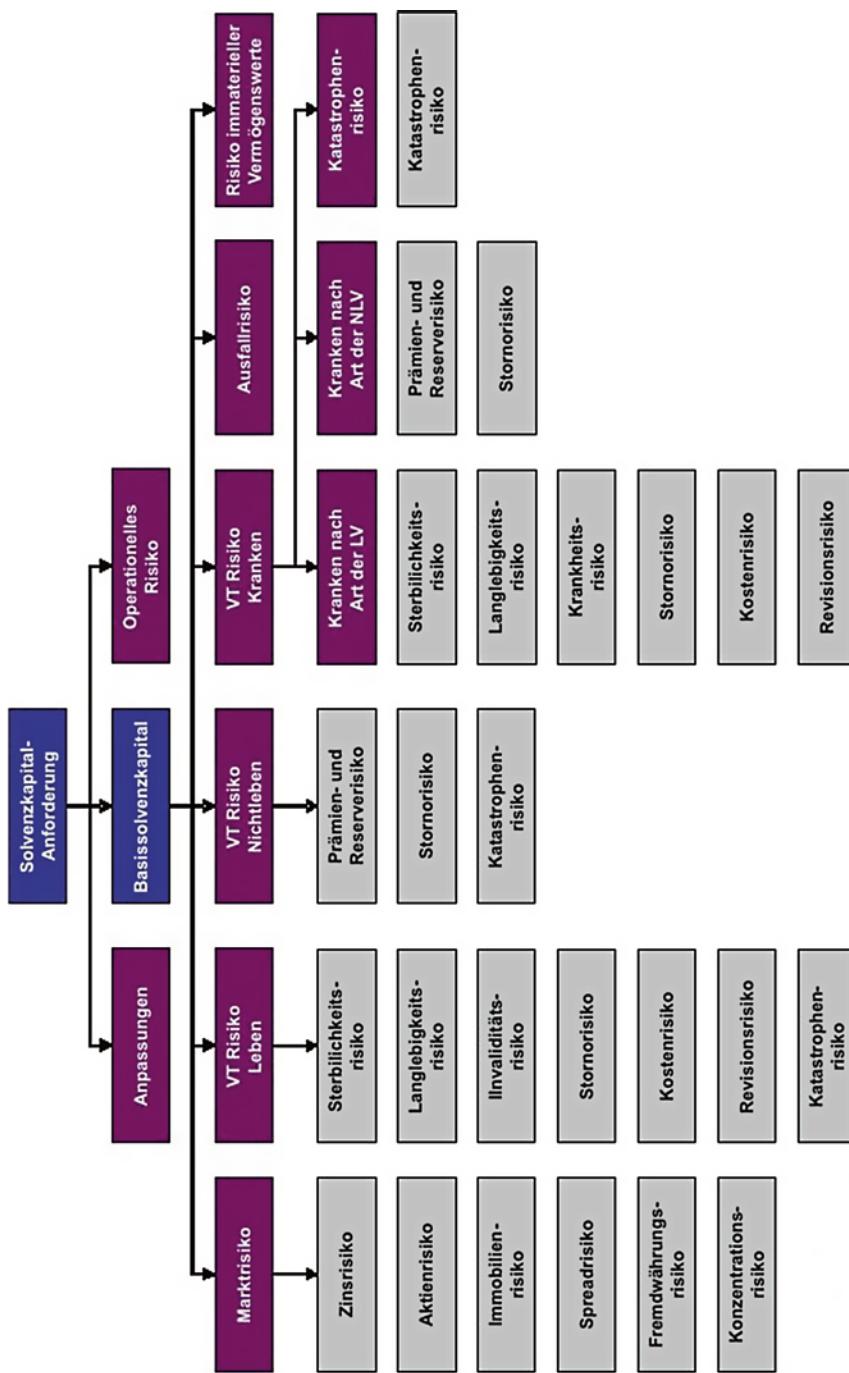


Abb. 33.5 Modulaufbau der Standardformel. (Quelle: eigene Darstellung in Anlehnung an Heep-Altiner o.J.)

SCR_i und SCR_j Risikomodule, Summe als Ausdruck aller möglichen Kombinationen von i und j (vgl. VAG, Anlage 3)

Die Risikomodule der Standardformel, aus denen sich das BSCR zusammensetzt (vgl. Heep-Altiner et al. 2014, S. 31), sind:

- **Marktrisiko:** Verlustrisiko aufgrund von Schwankungen der Marktpreise;
- **Gegenparteiausfallrisiko:** Verlustrisiko aufgrund von Kreditausfällen oder Bonitätsverschlechterungen von den Schuldern;
- **Versicherungstechnisches Risiko:** Risiko des technischen Ruins; die Risikomodule Nicht Leben, Leben und Kranken stellen das versicherungstechnische Risiko der einzelnen Sparten dar. Außerdem wird in jeder Sparte das Storno- und Katastrophenrisiko berücksichtigt;
- **Das Risiko immaterieller Vermögenswerte.**

Das operationelle Risiko ist nicht versicherungsspezifisch und in verschiedenen Branchen vorzufinden. Es umfasst die Möglichkeit von IT-Ausfällen und Managementfehlern.

Anders als in der Standardformel richtet sich das unternehmenseigen entwickelte interne Modell individuell an dem Versicherer aus. Nichtsdestotrotz muss das interne Modell von der BaFin genehmigt sein (vgl. BaFin 2016c). Die Tatsache, dass das Modell für die Risikolage des Unternehmens zugeschnitten ist und somit die Solvenzlage präziser bestimmt, spricht für die Entwicklung und Anwendung eines internen Modells. Dadurch kann ggf. höheres Eigenmittel ausgewiesen und die Position im Wettbewerb gestärkt werden (vgl. Heep-Altiner et al. 2015, S. 238). Weiterhin ist eine risikoorientierte Steuerung mithilfe des internen Modells besser möglich als bei der Nutzung der Standardformel. Bei der Auswahl eines Modells ist zu beachten, dass das interne Modell im Vergleich zur Standardformel mit mehr Zeitaufwand und Kosten verbunden ist. Das Unternehmen hat also abzuwegen, ob die Entwicklung und Anwendung des internen Modells langfristig profitabel sind.

Anders als bei der Standardformel verfolgt das interne Modell den Top-down-Ansatz. Es wird dementsprechend das Gesamt-SCR berechnet, ohne vorher einzeln auf die Risiken einzugehen. Der Kapitalbedarf wird dann auf die Risiken aufgeteilt. Die Höhe entspricht dem Anteil des Risikos in der gesamten Risikolage.

Aufgrund der hohen Komplexität und Aufwendung haben bisher nur einige wenige große Erst- und Rückversicherer ein internes Modell zertifizieren lassen (vgl. Bürger 2019):

- Allianz Gruppe,
- AXA Gruppe,
- Münchener Rückversicherung,
- Ergo,
- DKV,
- HDI Gruppe,
- Hannover Rück,
- E+S-Rück.

33.3.3 Säule 2: Qualitative Anforderungen

In der zweiten Säule erfolgt die Ergänzung der quantitativen Anforderungen der ersten Säule um qualitative Anforderungen. Diese beziehen sich auf die Einrichtung eines wirksamen Governance-Systems, das ein solides und vorsichtiges Management des Geschäfts gewährleistet. Versicherungsunternehmen haben gemäß Artikel 41 der SII-RRL (Solvency-II-Rahmenrichtlinie) ein Governance-System zu etablieren, das ein solides und vorsichtiges Management des Versicherungsgeschäfts ermöglicht. Hierfür wird die Einrichtung geeigneter Prozesse und Systeme verlangt, die vor allem das Risikomanagement, die unternehmenseigene Risiko- und Solvabilitätsbeurteilung (ORSA), die interne Kontrolle, die interne Revision, die versicherungsmathematische Funktion und das Outsourcing betreffen. Das Governance-System, das der Wesensart, dem Umfang und der Komplexität der Tätigkeiten des Versicherungsunternehmens angemessen sein muss (Proportionalitätsprinzip), unterliegt dem Überprüfungsprozess der Aufsichtsbehörde.

Besonders hervorgehoben werden kann der ORSA-Prozess. Der ORSA-Prozess beurteilt umfangreich die Risiko- und Solvabilitätslage eines Versicherungsunternehmens und dient als Überwachungsinstrument (vgl. Rohlfs 2018, S. 92). Gemäß § 27 VAG hat der Prozess als Teil des Risikomanagements die Aufgabe, das gesamte Risikoprofil zu bewerten und den entsprechenden Kapitalbedarf zu bestimmen. Die Versicherer sind dazu verpflichtet, diesen Prozess mindestens einmal jährlich durchzuführen. Auf diese Weise kann das Unternehmen unter anderem überprüfen, ob die Kapitalanforderungen und die Anforderungen an die versicherungstechnischen Rückstellungen eingehalten werden und „Abweichungen des tatsächlichen Risikoprofils von den Annahmen zur Ermittlung der Kapitalanforderungen“ (Langheid und Wandt 2017, Nr. 438) vorhanden sind.

Im Kern geht es darum, das unternehmenseigene Risikoprofil und den daraus resultierenden internen Risikokapitalbedarf kontinuierlich zu analysieren und zu bewerten, und zwar unabhängig von bzw. weitergehend zu der eigentlichen Ermittlung der Solvenzkapitalanforderung. Die Ergebnisse werden in einem ORSA-Bericht festgehalten.

33.3.4 Säule 3: Marktdisziplin und Berichtspflichten

Der dritten Säule werden die Marktdisziplin und Berichtspflichten zugeordnet. Diese Kriterien sollen die Transparenz innerhalb der Versicherungsbranche fördern (vgl. Rohlfs 2018, S. 94).

Die Berichterstattung wird nach den Adressaten unterschieden. Es gibt die Offenlegung gegenüber der Öffentlichkeit und gegenüber der Aufsicht. Zu der ersten Gruppe gehören der Solvency and Financial Condition Report (SFCR) und die Quantitative Reporting Templates (QRT). Beide Berichte sind auch für die Aufsicht bestimmt. Dazu gehören wei-

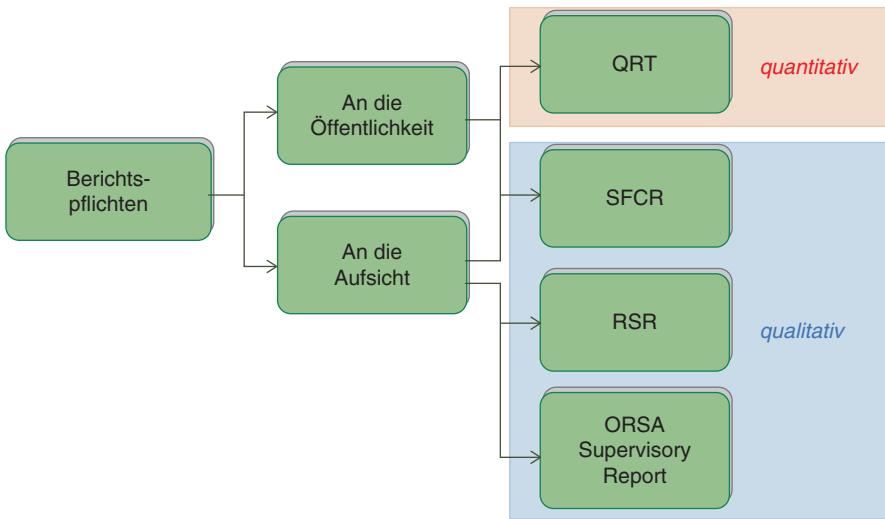


Abb. 33.6 Übersicht der Berichterstattung nach Solvency II. (Quelle: eigene Darstellung)

terhin der Regular Supervisory Reporting (RSR) und die ORSA Supervisory Report. Zudem sind qualitative Berichte von den quantitativen abzugrenzen. In Abb. 33.6 ist eine Übersicht der externen aufsichtsrechtlichen Risikoberichterstattung zu sehen.

Drei Berichte werden den qualitativen Berichtspflichten zugeordnet (vgl. Rohlf 2018, S. 95):

- **SFCR:** Der Solvabilitäts- und Finanzbericht informiert sowohl die Öffentlichkeit als auch die Aufsicht über die Risikolage und Solvabilität. In diesem Bericht wird unter anderem die Solvenzquote dokumentiert.
- **RSR:** Der reguläre Aufsichtsbericht ist nur für die Aufsicht zugänglich und weist eine größere inhaltliche Tiefe auf als der SFCR. Es werden unter anderem strategische Angaben und Unternehmensziele sowie detaillierte Informationen über die Solvenzlage offengelegt.
- **ORSA Supervisory Report:** Der ORSA Aufsichtsbericht wird im Rahmen der unternehmenseigenen Risiko- und Solvabilitätsbeurteilung erstellt und ist nur an die Aufsicht adressiert. Der Bericht enthält die Ergebnisse des ORSA-Prozesses.

Die quantitative Berichterstattung erfolgt regelmäßig unterjährig oder jährlich. Davon betroffen sind die Meldeformulare QRT (Quantitative Reporting Templates) (vgl. Rohlf 2018, S. 95). Die Meldeformulare stellen das SCR und MCR dar und sind die Grundlage zur Berechnung des Risikokapitalbedarfs und der Eigenmittel. Diese tragen zur Früherkennung von Risiken bei.

33.4 Vergleich zwischen Ratings und Solvency II

Im Folgenden werden die beiden Instrumente „Rating“ und „Solvency II“ verglichen. Dafür werden die positiven und negativen Aspekte beider Systeme aufgeführt und auf Gemeinsamkeiten und Unterschiede überprüft. Infolgedessen wird deren Wechselwirkung betrachtet.

33.4.1 Vor- und Nachteile des Ratingmodells

33.4.1.1 Vorteile

Wie bereits dargelegt, ist das Analysespektrum von Ratings sehr breit angelegt. Dadurch können Versicherungsunternehmen Ratings auch als internes Steuerungsinstrument nutzen. Führt man den Ratingprozess auch nach dem Erstrating in Form eines Folgeratings weiter, so dient das System auch als kontinuierliches Controllingverfahren für die Unternehmensführung. Durch den Einbezug eines breiten Analysespektrums, welches auch zukünftige Entwicklungen berücksichtigt, wirken Ratings im Zeitablauf als Stabilisator und Regulativ und schwanken nicht so stark wie SCR-Quoten.

Da ein Rating für den Emittenten eine Möglichkeit darstellt, Informationen aus dritter Hand über das jeweilige Unternehmen zu erhalten und auf dieser Grundlage eventuelle Investitionsentscheidungen zu treffen, kann sich eine positive Bewertung der externen Agenturen entsprechend positiv auf die Reputation des betroffenen Versicherungsunternehmens auswirken. Aus diesem Grund erfüllt das Rating in vielen Fällen auch die Funktion eines Marketinginstrumentes (vgl. Lürzer 2008, S. 10 ff.). Für die Versicherungsunternehmen bildet diese Bonitätsbeurteilung außerdem eine wichtige Entscheidungshilfe bei Kapitalfragen.

Des Weiteren spricht die einheitliche Vorgehensweise für die Ratingagenturen. Jede Beurteilung und jede Ratingvergabe laufen nach standardisierten Prozessen ab. Infolgedessen lassen sich die Rating-Noten branchenübergreifend gegenüberstellen und vergleichen, so dass Ratings den Emittenten zweckmäßig bei Investitionsfragen unterstützen.

Die Ratingagenturen unterliegen der unmittelbaren Aufsicht durch die europäische Wertpapierbehörde ESMA. Die Beaufsichtigung beginnt bereits vor der Registrierung als Ratingagentur durch ein „umfangreiches Prüfungs- und Genehmigungsverfahren“ (Goller 2013) und wird während der weiteren Geschäftstätigkeit durch regelmäßige Berichterstattungen fortgeführt. Mit der Zielrichtung, Transparenz und Stringenz im Markt zu fördern, unterliegen die Agenturen zahlreichen Anforderungen, welche auch die Qualität erhöhen.

33.4.1.2 Nachteile

Ratingagenturen sind in der Presse durchaus Kritik ausgesetzt. Da zumindest ein interaktiver Ratingprozess einen Auftrag des zu ratenden Unternehmens voraussetzt, welches eine Honorarzahlung an die Ratingagentur impliziert, steht häufig der Vorwurf im Raum,

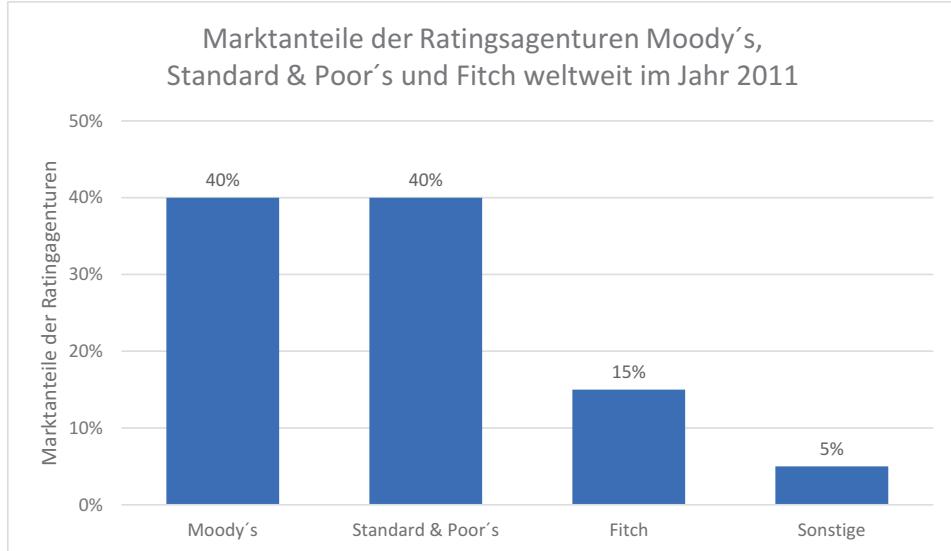


Abb. 33.7 Marktanteile der Ratingagenturen Moody's, Standard & Poor's und Fitch weltweit im Jahr 2011. (Quelle: eigene Darstellung in Anlehnung an Statista 2012)

dass die Ratingobjekte für ein gutes Rating bezahlen würden. Aus diesem Geschäftsmodell könnten demnach Interessenkonflikte folgen (vgl. Otte 2012). Obwohl die ESMA dem entgegenwirken soll, werden teilweise immer noch Interessenkonflikte hervorgehoben. Da Ratingagenturen gewinnorientierte Unternehmen sind, kommt in vielen Fällen der Verdacht von Missbrauch auf. Insbesondere die Objektivität der Ratingbranche wird dabei kritisiert.

Der Verdacht wird durch die quasi oligopolistische Marktstruktur weiter verstärkt. In Abschn. 33.2 wurden die fünf großen Ratingagenturen in der Versicherungsbranche dargestellt. Betrachtet man jedoch den Markt als Ganzes, das heißt weltweit und nicht nur auf Versicherungen beschränkt, teilten sich im Jahre 2011 die drei größten Ratingagenturen Moody's, Standard & Poor's (S&P) und Fitch 95 Prozent der Marktanteile (vgl. Abb. 33.7). Diese drei US-amerikanischen Unternehmen, auch „Big Three“ genannt, bewerten sowohl Unternehmen als auch Länder (vgl. Wente 2011).

Aufgrund dieser Konstellation wird häufig insbesondere in der Presse die Sorge geweckt, dass die „Big Three“ ihre Machtstellung missbrauchen könnten.

33.4.2 Vor- und Nachteile von Solvency II

33.4.2.1 Vorteile

Durch die Inkraftsetzung von Solvency II gelten zum ersten Mal EU-weit einheitliche Regeln für alle Mitgliedsstaaten (vgl. BaFin 2016b). Unter Solvency I galten die nationalen

Rechnungslegungsvorschriften, was einen innereuropäischen Vergleich der Versicherungsunternehmen deutlich erschwerte.

Eine bedeutende Neuerung durch Solvency II ist das Governance- und Risikomanagementsystem in der zweiten Säule. Mithilfe der geforderten Schlüsselfunktionen wird die Einrichtung angemessener und unternehmensfördernder „Entscheidungsprozesse und [...] Organisationsstruktur[en]“ (Rohlf 2018, S. 91) gefördert. Die Schlüsselfunktionen sorgen für eine stärkere Geschäftsorganisation, schenken wichtigen Funktionen eine höhere Bedeutung und stellen eine vollständige und angemessene Risikoerkennung sicher. Dabei wird das ganze Risikoprofil des Unternehmens auf allen Ebenen konsolidiert und fortlaufend durch den ORSA-Prozess überwacht.

Durch Solvency II hat auch die BaFin eine neue Positionierung in der Versicherungsbranche erfahren. Von jedem Versicherer verlangt die BaFin eine ausreichende Eigenmittelausstattung, um eine Solvenzunterschreitung zu verhindern. Das reformierte Regelwerk erlaubt es der Aufsicht, strenge Strafmaßnahmen zu verhängen, falls die Versicherer die aufsichtsrechtlichen Anforderungen nicht einhalten. Dies geht sogar so weit, dass die BaFin dem jeweiligen Versicherer die Geschäftstätigkeitserlaubnis entziehen kann. Diese Drohkulisse erhöht auf Seiten der Versicherer den Anreiz, den Anforderungen pflichtgemäß nachzukommen, um keine Konsequenzen zu erleiden (vgl. Querner 2016, S. 18).

Ein weiteres Ziel von Solvency II ist die Schaffung von Transparenz in der Versicherungsbranche. Dies behandelt insbesondere die dritte Säule und erfolgt in Form von verschiedenen Berichterstattungen. Wie bereits in Abschn. 33.3 erläutert, unterscheiden sich die Berichte nach Adressatengruppe und in ihrer Form. Die interne Berichterstattung ist von den externen zu differenzieren. Während die interne Berichterstattung, der Risikobericht, nur an den Vorstand kommuniziert, richtet sich die externe Berichterstattung an die Aufsichtsbehörden und die Öffentlichkeit. Behandelt werden dabei das Gesamtrisikoprofil und die Beurteilung der Risikosituation des Versicherers sowie wesentliche Änderungen und deren Folgen. Der Vorteil dabei ist, dass alle wesentlichen Bereiche ausgiebig zu überprüfen und zu dokumentieren sind. Der Risikobericht soll dem Vorstand einen umfassenden Einblick über die Gesamtlage des Versicherers ermöglichen. Daher werden zahlreiche Themen behandelt, wie zum Beispiel:

- Ziele des Risikomanagements,
- Bewertungsmethoden,
- Zielerreichung/-steuerung,
- Maßnahmen zur Risikosteuerung,
- Änderungen in der Geschäftspolitik.

Ein weiterer Vorteil des Berichtswesens ist, dass zwischen der Standard-Berichterstattung, die regelmäßig unterjährig oder jährlich stattfindet, und der Ad-hoc-Berichterstattung unterschieden wird. Somit lassen sich unternehmensgefährdende Entwicklungen rechtzeitig kommunizieren und bestmöglich reduzieren oder vermeiden. Die externe Berichterstattung bringt zudem den Vorteil der Vergleichbarkeit innerhalb des Versicherungsmarktes.

33.4.2.2 Nachteile

Solvency II hat allerdings auch Schwächen. Ein großer Kritikpunkt am jungen System ist seine Komplexität. Insbesondere die Standardformel wird diesbezüglich stark kritisiert. Die Berechnungen sind mit hohen Anforderungen verbunden und stellen eine immense zeitliche und finanzielle Belastung für die Unternehmen dar. Insbesondere kleinere und mittelständische Unternehmen haben Probleme, hierfür Ressourcen bereit zu stellen.

Die Standardformel wurde mit dem Ziel entwickelt, auf vereinfachte Weise eine Vergleichbarkeit im Versicherungsmarkt zu ermöglichen. Doch genau diese Vereinfachung ist der Grund dafür, dass die Ergebnisse teilweise nicht adäquat dargestellt werden können und lediglich beschränkte Interpretationen zulassen (vgl. Redaktion RiskNet 2011). Die Datenflut und die hohen Anforderungen gefährden die Intention der Markttransparenz und Vergleichbarkeit. Mithilfe des SFCR erhält die Öffentlichkeit Einblick in die Finanz- und Solvabilitätslage. Doch bei ca. 340 Versicherungsunternehmen, die Solvency II unterliegen, benötigt es sehr viel Zeit und Aufwand, die Menge an Informationen zu einem Vergleich auszuarbeiten und dieses Vorgehen jährlich zu wiederholen (vgl. ISS Software GmbH o. J.).

Doch nicht nur die hohen Anforderungen und der damit verbundene Arbeitsaufwand, sondern auch die vielen getroffenen Annahmen zur Bestimmung der Solvenzquote behindern die Vergleichbarkeit. Im Besonderen durch Prognosen zum Beispiel über die Kapitalanlagestruktur oder Überschussbeteiligung kann keine exakte Solvenzquote berechnet werden. Diese ist schließlich von vielen Einflussgrößen abhängig, wodurch eine Volatilität nicht zu verhindern ist (vgl. Kling 2017, S. 15 und 27).

Dies liegt insbesondere an der hohen Projektionsdauer. Die Berechnungen reichen bis zu 100 Jahre in die Zukunft und somit können die Einflussgrößen, wie zum Beispiel der Zins, große Schwankungen verursachen. Aufgrund der starken Volatilitäten dient die Solvenzquote hauptsächlich als Stichtagsbetrachtung (vgl. Dennstedt et al. 2016, S. 10).

Um den Versicherungsunternehmen einen reibungslosen Übergang von Solvency I zu Solvency II zu ermöglichen, hat der Gesetzgeber zwei Übergangsmaßnahmen vorgesehen (vgl. Aden et al. 2018, S. 8). Vor allen Dingen die Lebensversicherungsunternehmen machen hiervon Gebrauch, da der große Bestand an Verträgen mit hohen Garantiezinsversprechungen bei dem aktuell niedrigen Zinsniveau eine große Belastung für die Unternehmen darstellt.

Um die Übergangsmaßnahmen anwenden zu können, müssen die Versicherungsunternehmen eine Genehmigung bei der BaFin einholen. Die beiden Übergangsmaßnahmen richten sich auf die Rückstellungsbewertung. Die Regelungen sind in den §§ 351, 352 im VAG festgehalten und erlauben dem Versicherer, innerhalb von 16 Jahren stufenweise von der Solvency I-Bewertung auf die Solvency-II-Bewertung anzupassen. Hierdurch erhalten die Versicherer einen zeitlichen Aufschub, um sich auf die neuen Anforderungen einzulegen.

stellen und gleichzeitig die Auswirkungen besser zu steuern. Jedoch beeinflussen die Übergangsmaßnahmen auch die Höhe der Solvenzquote (vgl. Ermert 2016). So weisen Versicherer unter Anwendung der Maßnahmen eine höhere SCR-Quote aus als Versicherer ohne Bilanzierungshilfen.

Die Übergangsmaßnahmen und die Modelle zur Ermittlung des Solvenzkapitals erschweren die Vergleichbarkeit und Einheitlichkeit innerhalb des Versicherungsmarktes. Auch kann die SCR-Quote im Zeitablauf starken Schwankungen unterliegen. Falls Versicherer A sich für die Standardformel entscheidet und Übergangsmaßnahmen anwendet, Versicherer B jedoch mit einem internen Modell seine Solvabilität berechnet und bei der Bewertung der Rückstellungen auf Übergangsmaßnahmen verzichtet, ist ein Vergleich zwischen Versicherer A und B kaum möglich. Eine Betrachtung der Basis-SCR-Quoten (ohne Rückstellungstransitional und Volatilitätsanpassung) würde einen direkten Vergleich der Solvenzquoten der Versicherer ermöglichen, wobei auch hier Wahlrechte bei Kalibrierung der Modelle eine echte Vergleichbarkeit einschränken.

Außerdem ist die Rentabilität der Eigenmittel abhängig von der Gesellschaftsform des Versicherers. Bei einem Versicherungsverein auf Gegenseitigkeit sind die Versicherungsnehmer Mitglieder, so dass das Unternehmen die Gewinne einbehalten kann und dadurch mehr Eigenkapital ausweist.

33.4.3 Gemeinsamkeiten und Unterschiede

Sowohl die Standardformel von Solvency II als auch das Ratingverfahren sind externe Modelle. Beide Methoden verfolgen dabei das Ziel, eine Unterkapitalisierung frühzeitig zu erkennen. Auf diese Weise sollen sowohl Versicherungsnehmer als auch Kapitalgeber geschützt werden. Um dies zu bewerkstelligen, werden die quantitativen Anforderungen um qualitative Komponenten ergänzt. Mithilfe der Anforderungen soll sowohl im Ratingverfahren als auch bei Solvency II eine risikogerechte Unternehmensführung gewährleistet werden. Des Weiteren werden die Finanzkraft und Solvabilität des Versicherers bewertet. Diesbezüglich werden Informationen an die Öffentlichkeit berichtet, um die Transparenz innerhalb der Branche zu gewährleisten. Überwacht werden die Vorschriften in beiden Modellen von den jeweiligen Aufsichtsbehörden BaFin und ESMA.

Neben den Gemeinsamkeiten weisen die beiden Modelle aber auch Unterschiede auf. Das Rating bietet der Öffentlichkeit einen Gesamtüberblick. Mithilfe des Ratings kann die Bonität zwischen verschiedenen Ländern und branchenübergreifend weltweit verglichen werden. Die Solvenzquote bezieht sich hingegen nur auf die Versicherungsbranche und ist auf die EU beschränkt. Zudem sind die Versicherer dazu verpflichtet, die Anforderungen aus Solvency II zu erfüllen. Das Rating wird freiwillig von den Versicherern genutzt und basiert auf Honorarzahlungen.

33.4.4 Wechselwirkung

Nach der Gegenüberstellung von Solvency II und dem Ratingmodell gilt es nun zu untersuchen, in welcher Beziehung die beiden Systeme zueinander stehen. Herr Dr. Frank Grund, Exekutivdirektor der BaFin, hat in einem Interview im Juni 2016 in der Zeitschrift Versicherungswirtschaft auf die Frage, ob die Solvenzquote das Rating und dessen Aufgabe ersetzt, Stellung genommen:

„Ich hatte ursprünglich gedacht, Versicherer nutzen unter Solvency II keine Ratings mehr. Das scheint völlig falsch zu sein. Ich sehe vorerst keine Anzeichen dafür, dass die SCR-Quote die Rating-Urteile ablöst“ (Baltzer 2016, S. 23). Diese Ansicht lässt sich damit begründen, dass die beiden aufgeführten Systeme ähnliche Ziele, jedoch verschiedene Funktionen haben.

Die Solvenzquote trifft eine Aussage über den Bedeckungsgrad eines Unternehmens mit Eigenmitteln unter Berücksichtigung der Erfüllung des SCR. Ein Versicherer muss Risiken mit genügend Kapital hinterlegen. Da die Solvenzquote jährlich aufgrund ihrer Komponenten zu ermitteln ist, gibt der Wert nur den Status quo an. Eine langfristige Aussage über die Finanzkraft der Versicherer kann nur unter Berücksichtigung der Quote nicht getroffen werden. Dafür fehlt die Gesamtbeurteilung des Versicherungsunternehmens (vgl. Dennstedt et al. 2016, S. 11).

Das Rating beurteilt die Bonität des Versicherungsunternehmens. Hierzu werden alle Unternehmensebenen herangezogen. In Abschnitt 2 „Rating“ wurden die Schritte des Verfahrens genau beschrieben. Das Rating trifft Aussagen über die Kreditwürdigkeit des Ratingobjektes und dient den Investoren als Entscheidungshilfe. Dadurch wird die Ausfallwahrscheinlichkeit mithilfe verschiedener Kriterien bewertet. Eine genauere Analyse dieser Kriterien zeigt, dass bei der Beurteilung von Versicherungsunternehmen die SCR-Quote von Bedeutung ist. Ratings berücksichtigen, inwieweit die aufsichtsrechtlichen Anforderungen erfüllt werden. Im Besonderen beziehen die Agenturen bei der Beurteilung des Risikomanagements die Anforderungen von Solvency II und die Berichte, wie zum Beispiel den ORSA-Prozess und den ORSA-Bericht, ein.

Dies verdeutlicht die komplementäre Beziehung von Solvency II und Ratings. Gem. Art. 3 ff. Delegierte Verordnung wird der Bezug von Solvency II zu Ratings geregelt. Sie sind eine wichtige Bezugsgröße von Solvency II und werden in einzelnen Bereichen vorausgesetzt. Zum Beispiel sollten die Kapitalanlagerisiken durch Ratings dargestellt werden, anderenfalls müssen sie mit viel (mehr) Kapital unterlegt werden (vgl. Versicherungswirtschaft 2016, S. 18). Ratings finden nicht nur bei der Bewertung von Kapitalanlagerisiken Anwendung, sondern stellen auch eine wichtige Voraussetzung bei der Wahl des Rückversicherers dar. Mithilfe der Bonität wird die Wahrscheinlichkeit eines Rückversicherungsausfalls bewertet und eine Aussage zu der Kreditwürdigkeit des Rückversicherungsunternehmens getroffen (vgl. Heep-Altiner et al. 2014, S. 73). Die Wahl des

Rückversicherers ist davon abhängig, mit welcher Wahrscheinlichkeit dieser seinen Zahlungsverpflichtungen nachkommen kann.

Zudem werden Ratings im Vertrieb genutzt. Sie sind ein wichtiger Bestandteil der Produktberatung und werden häufig von Vermittlern verwendet. Auch in Werbeanzeigen werden Ratings in Form von Gütesiegeln genutzt, mit dem Ziel, als Versicherer vertrauenswürdig und zuverlässig aufzutreten.

Die Solvenzquote allein liefert keine vollständige Aussage, um die gesamte Finanzstärke eines Unternehmens zu beurteilen. Umgekehrt ist es den Versicherungsunternehmen nicht erlaubt, die Bonität ihre Kapitalanlagen nur auf Grundlage von Ratings zu ermitteln. Jedes Versicherungsunternehmen hat eigene Kreditrisikobewertungen durchzuführen, deren Interpretation durch Ratings ergänzt wird (vgl. BaFin 2017, B.3.1 c). Damit soll gemäß § 28 VAG die Abhängigkeit von Ratings verhindert und die Angemessenheit der berücksichtigten Ratings sichergestellt werden.

33.5 Fazit

In einem zusammenfassenden Fazit können folgende Leitfragen betrachtet werden:

1. Wie stehen Solvency II und das Ratingmodell zueinander?
2. Wird das Rating von der Solvenzquote vollkommen ersetzt?

Im Hinblick auf die Erkenntnisse, die in Abschn. 33.4 dargelegt worden sind, kann auf die erste Frage mit der gegenseitigen komplementären Beziehung zwischen den beiden Systemen geantwortet werden. Solvency II hat gegenüber Ratings eher einen komplementären Charakter, keinen substitutiven. Beide Modelle beeinflussen sich wechselseitig und gewährleisten den Aufbau und den Ablauf strukturierter sowie effektiver (risikoorientierter) Prozesse in der Versicherungswirtschaft.

Bezugnehmend auf die zweite Frage kann festgehalten werden, dass sowohl die Solvenzquote als auch Ratings in der Versicherungswirtschaft eine wichtige Rolle spielen. Ein Ersatz oder Ausschluss eines Modells durch das andere ist nicht möglich, denn gerade die Kombination beider Modelle ermöglicht eine optimale Bewertung der Risiko- und Finanzlage aus der Perspektive der Stakeholder. Die Aussage von (qualifizierten) Ratings ist nicht besser oder schlechter als die von Solvency II, sondern anders, da das Analysespektrum von Ratings in der Regel breiter angelegt ist. Die Rating-Note wird aus vielen Kriterien verdichtet und ist im Zeitablauf stabiler als einzelne Quoten. Ratings nehmen im Gegensatz zu SCR-Quoten für sich in Anspruch, die Messung von Sachverhalten mit einer Bewertung zu verbinden und spiegeln im Gegensatz zu SCR-Quoten „echte“ Abstufungen und Ausfallwahrscheinlichkeiten wider.

Literatur

- Aden, H., et al. (2018). Übergangsmaßnahmen sind integraler Bestandteil von Solvency II. In *Sozialversicherung in der Demografie- und Kostenfalle?!*, Aktuar aktuell, Hrsg. (Ausgabe 43, S. 8). Deutsche Aktuarvereinigung e. V. https://aktuar.de/fachartikelaktuaraktuell/AA43_%C3%9Cbergangsma%C3%9C%C3%9Fnahmen.pdf. Zugegriffen am 08.08.2019.
- ASSEKURATA Assekuranz-Rating Agentur GmbH. (o. J.). Bewertung versicherungstechnischer Verpflichtungen, Köln. solvency-ii-kompakt.de. <https://www.solvency-ii-kompakt.de/content/bewertung-versicherungstechnischer-verpflichtungen>. Zugegriffen am 08.08.2019.
- BaFin. (2016a). Eigenmittel und Eigenmittelanforderungen. bafin.de. https://www.bafin.de/DE/Aufsicht/VersichererPensionsfonds/Eigenmittelanforderungen/eigenmittelanforderungen_node.html. Zugegriffen am 22.08.2019.
- BaFin. (2016b). Solvency II. bafin.de. https://www.bafin.de/DE/Aufsicht/VersichererPensionsfonds/Aufsichtsregime/SolvencyII/solvency_II_node.html. Zugegriffen am 06.07.2019.
- BaFin. (2016c). *Interne Modelle in der Versicherungswirtschaft: Laufende Aufsicht über interne Modelle unter Solvency II*. Beitrag aus dem Jahresbericht 2016 der BaFin. https://www.bafin.de/DE/PublikationenDaten/Jahresbericht/Jahresbericht2016/Kapitel2/Kapitel2_8/Kapitel2_8_2/kapitel2_8_2_node.html. Zugegriffen am 09.07.2019.
- BaFin. (2017). Rundschreiben 11/2017 (Versicherungsaufsicht). bafin.de, B.3.1 c). https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1711_hinweise_anlage_sicherungsvermoegen_va.html. Zugegriffen am 08.08.2019.
- Baltzer, C. (2016). Eine absolute Garantie kann kein System bieten. *Versicherungswirtschaft*, 6, 22–23.
- Blaß, R. (2018). External Credit Assessment Institution. gabler-banklexikon.de. <https://www.gabler-banklexikon.de/definition/external-credit-assessment-institution-81856>. Zugegriffen am 13.08.2019.
- Bürger, T. (2019). Wie Versicherungen das Mammutregelwerk stemmen. private-banking-magazin.de. <https://www.private-banking-magazin.de/drei-jahre-solvency-ii-wie-versicherungen-das-mammutregelwerk-stemmen/>. Zugegriffen am 19.08.2019.
- Dennstedt, N., et al. (2016). Solvenzquote – Eine Momentaufnahme mit beschränkter Aussagekraft. In *Solvency II – Eine neue Ära hat begonnen!*, Aktuar aktuell, Hrsg. (Sonderausgabe, S. 10–11). Deutsche Aktuarvereinigung e. V. https://aktuar.de/fachartikelaktuaraktuell/AA32_Solvabilitätsquote.pdf#page=2&zoom=auto,-107,466. Zugegriffen am 11.07.2019.
- Dudenredaktion. (Hrsg.). (o. J.). Risiko, das. Duden online. <https://www.duden.de/rechtschreibung/Risiko>. Zugegriffen am 25.08.2019.
- Durchführungsverordnung (EG) 2016/1800 der Kommission. (2016). zur Festlegung technischer Durchführungsstandards im Hinblick auf die Zuweisung der Ratings externer Ratingagenturen zu einer objektiven Skala von Bonitätsstufen gem. der Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates, Anhang S. 4. <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R1800&from=EN>. Zugegriffen am 12.08.2019.
- Ermert, O. (2016). Solvency II: Übergangsmaßnahmen zur Rückstellungsbewertung – Eine erste Bestandsauftnahme. bafin.de. https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2016/fa_bj_1603_lebensversicherer.html. Zugegriffen am 10.08.2019.
- Goller, B. (2013). Ratingagenturen unter ESMA-Aufsicht. bafin.de. https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2013/fa_bj_2013_01_ratingagenturen.html. Zugegriffen am 12.08.2019.
- Gründl, H., & Kraft, M. (Hrsg.). (2019). *Solvency II – Eine Einführung. Grundlagen der neuen Versicherungsaufsicht* (3. Aufl.). Karlsruhe: Versicherungswirtschaft GmbH.

- Heep-Altiner, M. (o. J.). Vom Standardmodell zur integrierten Risikosteuerung, Köln. solvency-ii-kompakt.de. <https://www.solvency-ii-kompakt.de/content/vom-standardmodell-zur-integrierten-risikosteuerung>. Zugegriffen am 12.07.2019.
- Heep-Altiner, M., et al. (2014). *Wertorientierte Steuerung in der Schadenversicherung: Schritt für Schritt zur wert- und risikoorientierten Unternehmenssteuerung*. Karlsruhe: Versicherungswirtschaft GmbH.
- Heep-Altiner, M., et al. (2015). *Finanzierung im (Schaden-)Versicherungsunternehmen: Schritt für Schritt zu den Finanzierungsanforderungen eines (Schaden-) Versicherungsunternehmens*. Karlsruhe: Versicherungswirtschaft GmbH.
- ISS Software GmbH. (o. J.). Solvency II: Transparenz nur für Experten? solvency-ii-kompakt.de, Hamburg. <https://www.solvency-ii-kompakt.de/content/solvency-ii-transparenz-nur-fuer-experten>. Zugegriffen am 19.08.2019.
- Kling, A. (2017). *Solvency II = Spaghetti Bolognese? Die Auswirkungen von Solvency II und deren Bedeutung*. Stuttgart: Institut für Finanz- und Aktuarwissenschaften. https://www.ifa-ulm.de/fileadmin/user_upload/download/vortraege/2017_ifa_Kling_Solvency-II-Spaghetti-Bolognese-Die-Auswirkungen-von-Solvency-II-und-deren-Bedeutung_Forum-2017-Stuttgarter-Versicherung.pdf. Zugegriffen am 04.08.2019.
- Langheid, T., & Wandt, M. (2017). *Risikomanagement/ORSA, Münchener Kommentar zum VVG* (2. Aufl.). München: C.H.BECK, Nr. 435–439.
- Lürzer, R. (2008). Ratings von Versicherungsunternehmen: Hintergründe, Nutzen und Vorgehen beim Erstrating, Trendmonitor 4-2008. *Fokus thema*, 2, 10–13. <http://www.gcn.at/downloads/MI-04-2008F2.pdf>. Zugegriffen 06.08.2019.
- Otte, M. (2012). Rating-Agenturen. bpb.de. <https://www.bpb.de/politik/wirtschaft/finanzmaerkte/133275/rating-agenturen?p=all>. Zugegriffen am 12.08.2019.
- Querner, I. (2016). *Workshop: Wie Funktioniert Solvency II? Und was folgt daraus?* Frankfurt am Main: GDV. <https://www.gdv.de/resource/blob/8986/2cf2fa7c74a4d24cd444e8129ff17818/%2D%2D-zur-pr-sentation%2D%2D1690870317-data.pdf>. Zugegriffen am 03.08.2019.
- Redaktion RiskNet. (2011). QIS5-Ergebnisse veröffentlicht: Kritik an Komplexität der Standardformel von Solvency II. risknet.de. <https://www.risknet.de/themen/risknews/kritik-an-komplexitaet-der-standardformel-von-solvency-ii/>. Zugegriffen am 07.08.2019.
- Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates. (2009). Betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit (Solvabilität II), Neufassung, Art. 44, Abs. 1. <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32009L0138>. Zugegriffen am 25.08.2019.
- Rohlfs, T. (2018). *Risikomanagement im Versicherungsunternehmen: Identifizierung, Bewertung und Steuerung*. Karlsruhe: VVW GmbH.
- Statista. (2012). Marktanteile der Ratingagenturen Moody's, Standard & Poor's und Fitch weltweit im Jahr 2011. [de.statista.com. https://de.statista.com/statistik/daten/studie/199155/umfrage/marktanteile-der-drei-grossen-ratingagenturen-weltweit/](https://de.statista.com/statistik/daten/studie/199155/umfrage/marktanteile-der-drei-grossen-ratingagenturen-weltweit/). Zugegriffen am 12.08.2019.
- Verordnung (EG) 1060/2009 des Europäischen Parlaments und des Rates. (2009). Ratingagentur, Art. 3 Abs. 1a. <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32009R1060&from=LV>. Zugegriffen am 12.08.2019.
- Versicherungsmagazin. (o. J.). Public information rating. <https://www.versicherungsmagazin.de/lexikon/public-information-rating-1986028.html#definition>. Zugegriffen am 09.07.2019.
- Versicherungswirtschaft. (2016). Titelreport: Aufpasser, Heft 6, S. 18–21.
- Wente, S. (2011). Die „Big Three“ der Ratingagenturen. anlegerplus.de. <https://anlegerplus.de/home/die-big-three-der-ratingagenturen/>. Zugegriffen am 12.08.2019.

Hüseyin Kaya schloss nach seiner Ausbildung zum Versicherungskaufmann bei einem großen Kölner Versicherungskonzern mehrere Studien unter anderem in Betriebswirtschaftslehre und Insurance Science an der Universität zu Köln und an der Technischen Hochschule Köln ab. Bei der ASSEKURATA Assekuranz Rating-Agentur GmbH in Köln ist er als Senior-Analyst und Projektleiter an zahlreichen Ratings beteiligt. In seiner Funktion als Fachkoordinator Kapitalanlage/Risikomanagement verantwortet Herr Kaya darüber hinaus die Pflege und Weiterentwicklung aller Ratingtools und -modelle im Kapitalanlage-/Risikomanagementbereich und leitet ein Team von Fachspezialisten.

Mergime Rahimi studierte dual Versicherungswesen mit den Schwerpunkten Risk Management, Versicherungsmathematik und Marketing am Institut für Versicherungswesen der Technischen Hochschule Köln. Ihre Ausbildung zur Kauffrau für Versicherungen und Finanzen absolvierte Frau Rahimi bei dem Continentale Versicherungsverbund. Aktuell arbeitet sie bei EY in Köln im Bereich Tax Technology and Transformation.



Herausforderungen bei der Schadenregulierung

34

Birgit Beudt und Frank Cremer

Zusammenfassung

Die Welt wird durch die zunehmende Globalisierung und durch stetig wechselnde rechtliche Landschaften komplexer. Diese Entwicklungen beeinflussen auch die Schadenbearbeitung von Industriever sicherungsverträgen. Vor diesem Hintergrund beschäftigt sich das Kapitel mit den Herausforderungen, denen der Versicherungsnehmer in der Schadenregulierung ausgesetzt ist, und zeigt entsprechende Handlungsempfehlungen auf. Beginnend mit der Auswahl des Versicherers gliedert es sich in die zeitlichen Dimensionen „vor dem Schaden“, „während des Schadens“ und „nach dem Schaden“ sowie einen „Ausblick“. Im ersten Abschnitt „Schadenbearbeitung als ein Kernprozess des Versicherers“ wird dem Leser verdeutlicht, warum eine sorgfältige Überprüfung des Versicherers wichtig ist und welche Auswahlkriterien eine Rolle spielen. Im nächsten Abschnitt werden Handlungsempfehlungen herausgearbeitet, die vom Versicherungsnehmer bereits vor dem Schaden zu berücksichtigen sind, um später dann eine zügige und zufriedenstellende Regulierung zu gewährleisten. In der zeitlichen Dimension „während des Schadens“ erfolgt eine Darstellung der Beteiligten im Schadensprozess, der ersten Schritte einer Schadensmeldung, einzuleitender Ad-hoc-Maßnahmen sowie Ausführungen zur Bedeutung der Krisenkommunikation und zu den Obliegenheiten im Schadensfall. Der vierte Abschnitt behandelt das Schadencontrolling und

B. Beudt

Die Versicherergemeinschaft für Steuerberater und Wirtschaftsprüfer, Wiesbaden, Deutschland
E-Mail: Birgit.Beudt@v-s-w.de

F. Cremer (✉)

TH Köln, Institut für Versicherungswesen, Köln, Deutschland
E-Mail: frankcremer@email.de

Empfehlungen, wie das Unternehmen nach dem Schadensfall zu einer positiven Reputation beitragen kann. Zukünftige Trends und Innovationen bilden den Abschluss.

34.1 Schadenbearbeitung als ein Kernprozess des Versicherers – Auswahlkriterien

In einem Schadensfall, dem „Moment of Truth“ in der Vertragsbeziehung zwischen Versicherer und Versicherungsnehmer, zeigt sich, ob der Versicherer die Erwartungen des Versicherungsnehmers und das in ihn gesetzte Vertrauen erfüllt. Die besten und individuell auf das Unternehmen zugeschnittenen Vertragskonditionen sind wirkungslos, wenn sich der Ablauf der Schadenbearbeitung zeitlich verzögert, unprofessionell durchgeführt wird, unberechtigte Schadenersatzansprüche nicht erfolgreich abgewehrt werden oder der begehrte Deckungsschutz vom Versicherer versagt wird (vgl. Munkwitz 2015, S. 4). Bereits mit der Auswahl seines Versicherers stellt der Versicherungsnehmer dabei die ersten Weichen für eine erfolgreiche und adäquate Schadenregulierung.

Aufgrund zunehmender Globalisierung und ständiger gesetzlicher Neuerungen werden die heutigen Schadensfälle immer komplexer. Dies erfordert eine entsprechende fachliche Kompetenz der Schadenbearbeiter, um nicht in jedem Schadenfall einen Sachverständigen/Experten hinzuziehen zu müssen. Aber auch ein reibungsloser, unbürokratischer und schneller Ablauf der Schadenregulierung kann für das einzelne Unternehmen existenzentscheidend sein. Vor diesem Hintergrund wird deutlich, wie wichtig die sorgfältige Auswahl des Versicherers ist, und dass als Auswahlkriterium nicht allein die Höhe der Versicherungsprämie ausschlaggebend sein darf.

Die Regulierung von Großschäden sollte zum täglichen Geschäft des Versicherers gehören, in dessen Rahmen er auf ein bestehendes Netzwerk zurückgreifen kann, um allen Anforderungen bei der Schadenregulierung gerecht zu werden.

Eine gute und zeitnahe Kommunikation geprägt durch Attribute wie Erreichbarkeit und Termintreue zwischen Versicherer und Versicherungsnehmer ist im Schadenfall eine Grundvoraussetzung für eine Schadenregulierung, die auch die Bedürfnisse und Interessen des Versicherungsnehmers ausreichend berücksichtigen sollte, ohne an im Einzelfall notwendiger Flexibilität zu sparen. Im Industriever sicherungsbereich hat sich bewährt, dass persönliche Ansprechpartner (zum Beispiel Key-Account Manager) für den Versicherungsnehmer zur Verfügung stehen. Denn durch einen regelmäßigen und konstruktiven Austausch können wichtige Maßnahmen im Schadenfall schneller eingeleitet werden, mit dem positiven Effekt, dass der Schaden und auch die dazugehörigen Kosten reduziert werden können. Die direkte Kundenbeziehung, kurze Abstimmungswege und vertiefte Vertragskenntnisse gewährleisten eine Win-Win-Situation für beide am Schaden beteiligten Parteien.

Kritisch zu hinterfragen ist hingegen die Zusammenarbeit mit einem Versicherungsunternehmen, dessen Schadenabteilung gänzlich ausgliedert ist. Dies birgt nicht zuletzt

die Gefahr, dass der Regulierungsprozess unnötig verzögert wird, wenn zum Beispiel Klärungsbedarf hinsichtlich der Anwendung oder Auslegung von Bedingungen besteht, was nicht selten der Fall ist.

34.2 Vor dem Schaden

34.2.1 Risikoanalyse des Versicherungsnehmers

Das zu versichernde Unternehmen benötigt im ersten Schritt eine umfassende Risikoanalyse seiner individuellen Unternehmensrisiken und des bereits bestehenden Versicherungsschutzes. Im zweiten Schritt müssen die Beurteilung und Bewertung der notwendigen Versorgungslage folgen. Anhand einer solchen Analyse kann das Unternehmen dann entscheiden, welche Risiken es selbst tragen möchte und welche Risiken durch den Abschluss eines Versicherungsvertrages auf den Versicherer transferiert werden sollen. Voraussetzung für diese notwendige Risikoanalyse ist eine valide und vollständige Datenbasis über alle Risiken und in der Vergangenheit eingetretenen Schäden (vgl. Rohlfs 2018, S. 97).

34.2.2 Schadenpräventionsmaßnahmen

Die Schadenprävention hat eine besondere Bedeutung, da sie einerseits Schäden vermeidet und dafür sorgt, dass der Versicherer kritische Risiken (zum Beispiel Papier- und Chemieindustrie) auch versichert. Darüber hinaus können Präventionsmaßnahmen, die über gesetzlichen Anforderungen hinausgehen, in Vertragsverhandlungen ein gewichtiges Argument für eine Prämie im unteren Risikobereich sein. Versicherer und auch manche Versicherungsmakler beraten darüber hinaus zu den Optimierungsmöglichkeiten in Bezug auf individuelle Maßnahmen zur Schadenprävention des Unternehmens.

Die folgenden aufgelisteten Fragestellungen dienen der Anregung zu Präventionsmaßnahmen und sind selbstverständlich nicht abschließend:

Brandschutz

Sind geeignete Brandmelde- und Löschanlagen, Blitz- und Überspannungsschutzsysteme installiert? Wurden anhand vorher festgelegter Routinen diese kontinuierlich und auf Einsatzbereitschaft überprüft?

Naturgefahren

Sind Unternehmensstandorte und Produktionsprozesse so geplant und gesteuert, dass angemessene präventive Maßnahmen eingeleitet werden können?

- Beispiel „Hochwasser-Pass“: Damit kann das individuelle Gefährdungspotenzial aufgezeigt und geeignete Hochwasserschutzanlagen (zum Beispiel Deich, Schutzmauer,

Rückhaltebecken), die das Risiko Starkregen, Hochwasser, Hagel, Sturm minimieren (vgl. Hochwasser – Risiken für Unternehmen 2016, S. 2 bis 3), installiert werden.

- Beispiel „Erdbeben in Japan“: Die Vernachlässigung derartiger Risiken (landestypischer Gefahren) kann kritische Störungen von Lieferketten verursachen, die in eine Betriebsunterbrechung münden können. Diese als Rückwirkungsschäden bezeichneten Schadensfälle sind die Folge eines Sachschadens im Zulieferer-Unternehmen. Durch deren Abhängigkeit erleidet das Abnehmer-Unternehmen einen Unterbrechungsschaden, ohne dass es selbst von einem Sachschaden betroffen ist. Rückwirkungsschäden können sich beim Abnehmer-Unternehmen als auch beim Zulieferer-Unternehmen ereignen.

Maschinendefekt und Arbeitsschutz

Werden Gebäude und technische Anlagen regelmäßig gewartet und in regelmäßigen Abständen etwaige Anpassungen bzw. Neuerungen aktualisiert? Wird der gesetzlich vorgeschriebene Arbeits- und Gesundheitsschutz eingehalten? Kann darüber hinausgehender Arbeits- und Gesundheitsschutz sichergestellt werden?

Security

Ist ein ausreichender Einbruchschutz durch zum Beispiel einbruchhemmende Türen und Fenster, innenseitig montierte Rollläden, Videoüberwachung, ausreichende Beleuchtung sowie qualifizierte Alarmanlagen vorhanden?

Cyber

Wurden die vielfältigen Möglichkeiten der Schadenprävention in diesem Bereich ausreichend genutzt? Beispiele: Einsatz einer Firewall, Virenscanner, Regelung zum Umgang mit Emails unbekannter Absender sowie die Erteilung von notwendigen Zugangsrechten, wöchentliche Datensicherungen (je öfter desto besser), Passwortsicherung von mobilen Geräten und Regelung zur Verhinderung von Manipulationen von Sicherungskopien. Stehen im Falle eines Cyberangriffs IT-Dienstleister zur Verfügung, um direkt Gegenmaßnahmen einzuleiten oder anhand von IT-Forensik zur Aufklärung des Datendiebstahls beitragen zu können? Ist die Nutzung von Cloud Computing oder die Einrichtung einer externen Datensicherung sinnvoll?

Datenschutz und Compliance

Werden personenbezogene Daten gemäß der seit dem 25. Mai 2018 bestehende DSGVO verarbeitet? Existiert ein funktionierendes System, das eine korrekte Ausübung der Rechtsordnung ermöglicht und sicherstellt? Werden die Rechte der Betroffenen in einem Schadensfall gewahrt?

In der Gesamtschau sollte die Auseinandersetzung mit vorhandenen und neuen Schadenpräventionsmaßnahmen auch zu einer Schärfung des Risikobewusstseins bei der Unternehmensleitung und bei den Mitarbeitern führen, so dass Fehlentwicklungen bei Schadenpräventionsmaßnahmen nicht durch den nachträglichen Einkauf von Versicherungslösungen korrigiert werden können und sollen.

34.2.3 Unterteilung und Besonderheiten der Schadenversicherung

Sachversicherung

In der Sachversicherung ist das Sachsubstanzinteresse des Unternehmens (also Versicherung von Sachwerten gegen Zerstörung, Beschädigung, Abhandenkommen versicherter Sachen, wie zum Beispiel Gebäude, technische und kaufmännische Betriebseinrichtung, Vorräte etc.) gedeckt. Häufig sind die versicherten Gefahren im Versicherungsvertrag explizit genannt und/oder die nicht versicherten Gefahren in den Ausschlüssen aufgeführt. Eine Besonderheit in der Regulierung der Sachversicherung ist der Neuwertersatz (Ausnahmen möglich). Beim Neuwert wird der Betrag ersetzt, den die betroffene Sache zum Zeitpunkt des Schadens neu kostet (vgl. Munkwitz 2015, S. 4). Wichtige Sparten dieses Versicherungszweigs sind die Gebäude-, Maschinen-, Betriebsunterbrechungs- sowie die Transportversicherung (vgl. Abb. 34.1).

Rechtsschutzversicherung

Die Rechtsschutzversicherung erstattet und vermittelt Dienstleistungen zur Wahrnehmung der rechtlichen Interessen des Versicherungsnehmers (Abwehr und Durchsetzung von Ansprüchen, strafrechtliche Verteidigung und Beratung). Versichert sind die Rechtskosten bis zur Höhe der vereinbarten Versicherungssumme. Beispiele für Kostenübernahmen durch den Versicherer sind die telefonische anwaltliche Erstberatung zur Vorsorge, außergerichtliche und gerichtliche Rechtsanwaltsgebühren, Gerichtskosten und Kosten für außegerichtliche Streitschlichtungsverfahren.

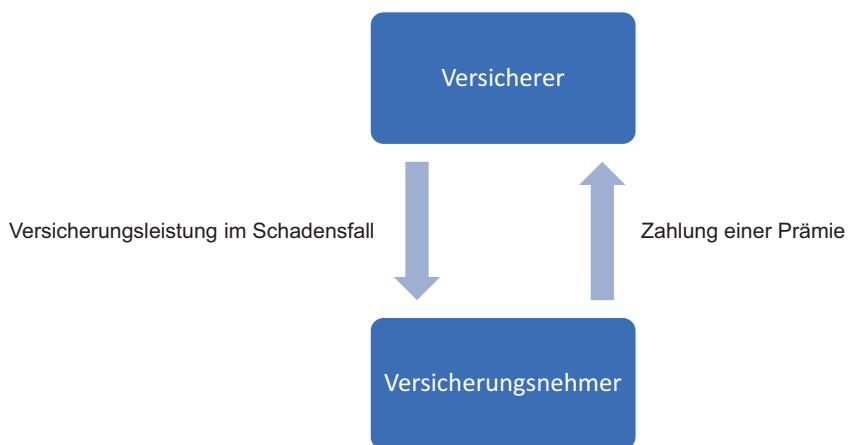


Abb. 34.1 Schadenregulierung in der Sachversicherung. (Quelle: eigene Darstellung)

Haftpflichtversicherung

Eine Haftpflichtversicherung bietet grundsätzlich das Prüfen der Haftpflichtfrage, die Abwehr unberechtigter Ansprüche Dritter (Rechtsschutzfunktion) sowie die Befriedigung berechtigter Schadenersatzansprüche Dritter (Zahlungsfunktion) gegenüber dem Versicherungsnehmer (Dreiecksverhältnis; vgl. Abb. 34.2) (vgl. Munkwitz 2015, S. 4).

Eine Besonderheit in der Schadenregulierung bei der Haftpflichtversicherung ist der Ersatz der beschädigten Sache zum Zeitwert. Beim Zeitwert (Stichwort: Wertverlust „neu für alt“) wird der Wert der Sache ersetzt, der zum Zeitpunkt des Schadens unter Berücksichtigung des Alters und der Abnutzung der Sache besteht (in Anlehnung an § 287 ZPO, Entscheidung des Gerichtes unter Einbeziehung aller Umständen nach freier Überzeugung) (vgl. Munkwitz 2015, S. 4). Zu den bekanntesten Versicherungen in diesem Kontext gehört die Betriebshaftpflichtversicherung.

Vor diesem Hintergrund ist die Regulierung eines Schadens für den Versicherungsnehmer, sofern eine Wahlmöglichkeit besteht, über eine Sachversicherung wirtschaftlich günstiger als über eine Haftpflichtversicherung (vgl. Munkwitz 2015, S. 4).

34.2.4 Gestaltung des Versicherungsvertrages

Im Rahmen der Vertragsverhandlungen können Versicherungsnehmer und Versicherer maßgeblich dazu beitragen, wie erfolgreich und zufriedenstellend eine spätere Schadenregulierung verläuft. Zu beachten ist, dass die Beschränkungen der Vertragsfreiheit durch halbzwangende oder zwingende Vorschriften nicht für Großrisiken gemäß § 210 VVG gelten. Diese Schutzfunktion (entwickelt für den durchschnittlichen Versicherungsnehmer) entfällt, da sich die Parteien auf Augenhöhe bei der Vertragsgestaltung befinden und sich aufgrund der Geschäftserfahrung ausreichend selbst schützen können (vgl. Rüffer et al. 2015, § 210). Zu den Großrisiken zählen Unternehmen, die nach dem VVG zwei der drei Merkmale aufweisen:

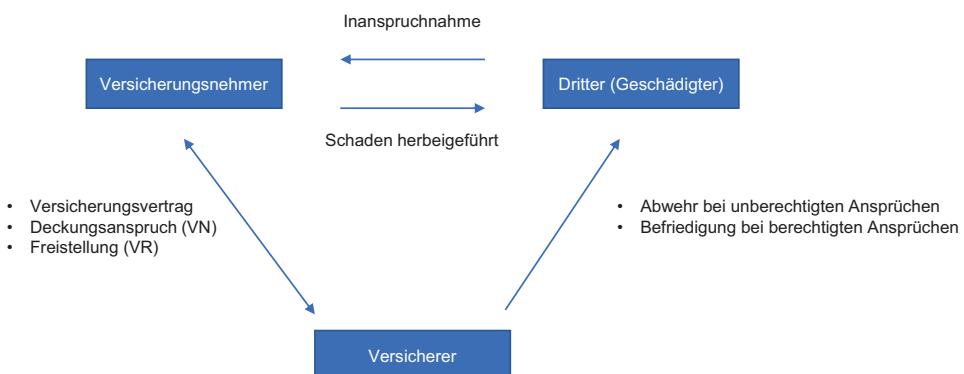


Abb. 34.2 Schadenregulierung in der Haftpflichtversicherung. (Quelle: eigene Darstellung)

- 6.200.000,00 Euro Bilanzsumme
- 12.800.000,00 Euro Nettoumsatzerlöse
- im Durchschnitt 250 Arbeitnehmer pro Wirtschaftsjahr.

Nachfolgend wird auf ausgewählte Punkte, die bei einer Gestaltung des Vertrages aufmerksam betrachtet werden sollten, eingegangen.

34.2.4.1 Vorvertragliche Anzeigepflicht

Um ein genaues Bild über das Risiko zu erhalten, muss das zu versichernde Unternehmen vor Vertragsabschluss alle Fragen des Versicherers im Rahmen eines Antrages bzw. Fragebogens beantworten. Diese Angaben werden benötigt, damit das Versicherungsunternehmen entscheiden kann, ob und unter welchen Bedingungen das Risiko versichert werden kann. Der Versicherungsnehmer sollte sich darüber bewusst sein, dass er im Rahmen seiner Anzeigepflicht gemäß § 19 VVG alle Fragen wahrheitsgemäß und vollständig beantworten muss. Gemäß § 19 Abs. 5 VVG muss der Versicherer den zukünftigen Versicherungsnehmer auf diese Pflichten und auf deren Rechtsfolgen bei Verletzung in Textform hinweisen. Selbstverständlich sind Gefahrenumstände, von denen der Versicherungsnehmer zum Zeitpunkt der Antragsstellung keine Kenntnis hatte, von dieser Anzeigepflicht ausgeschlossen.

Verletzt der Versicherungsnehmer die vorvertragliche Anzeigepflicht kann dies zur Folge haben, dass

- der Versicherer vom Versicherungsvertrag zurücktritt
- der Versicherer den Versicherungsvertrag innerhalb eines Monats kündigt
- im Schadensfall keine Versicherungsleistung durch den Versicherer erbracht werden muss
- der Versicherer den Vertrag mit neuen Bedingungen anpasst
- die Versicherungsprämie entsprechend dem tatsächlichen Risiko erhöht wird.

All diese Rechtsfolgen ziehen nicht nur eine mögliche Deckungslücke im Versicherungsschutz nach sich, sondern verursachen auch erhebliche Mehrarbeit beim Versicherungsnehmer im Rahmen der Wiederherstellung des uneingeschränkten Versicherungsschutzes.

34.2.4.2 Vorausschauende Klauseln

Unterschiedliche Vorstellungen vom Versicherungsschutz zwischen Versicherer und Versicherungsnehmer führen nicht selten zu zusätzlichen, zeitaufwendigen und unnötigen Konflikten innerhalb der Schadenregulierung. Der Grund dafür liegt oftmals in missverständlich formulierten bzw. fehlenden Vertragsklauseln (vgl. Becker 2015, S. 28). Vorbeugend sollte daher individuell geprüft werden, welche vorausschauenden Klauseln in den Versicherungsvertrag einzubeziehen sind. Nachfolgend wird auf eine ausgewählte Reihe an Versicherungsklauseln eingegangen:

Führungsklausel

Bei industriellen Risiken, deren Versicherungssummen häufig im zwei- oder sogar dreistelligen Millionenbereich liegen, sind in der Regel aus Kapazitätsgründen mehrere Versicherer beteiligt (vgl. Becker 2015, S. 28). Das gesamte Versichererkonsortium müsste im Versicherungsfall für den jeweiligen Risikoanteil am Konsortium die Schadensregulierung durchführen. Dass dies nicht sinnvoll ist, liegt auf der Hand. Die Lösung ist die Vereinbarung einer Führungsklausel. Anzeigen und Willenserklärungen des Versicherungsnehmers werden dann nur gegenüber dem „führenden“ Versicherer abgegeben, mit verbindlicher Wirkung auch für die anderen beteiligten Versicherer. Alle Entscheidungen des führenden Versicherers erkennen die beteiligten Versicherer als rechtsverbindlich für ihren Risikoanteil an und haften als Einzelschuldner im jeweiligen Verhältnis ihrer Anteile. Damit wird die Schadenregulierung (trotz des bestehenden Konsortiums) nur durch einen Versicherer durchgeführt. Der Versicherungsnehmer muss nur mit diesem Versicherer interagieren und sich abstimmen. Auch im Falle aus dem Versicherungsvertrag entstehender Rechtsstreitigkeiten ist der „Führende“ allein Prozesspartei und prozessführungsbefugt. Im Rahmen eines Deckungsprozesses muss der Versicherungsnehmer seinen Anspruch nur gegen den führenden Versicherer bzgl. dessen Risikoanteils gerichtlich geltend machen. Die beteiligten Versicherer akzeptieren die rechtskräftig ergangene Entscheidung auch für sich als bindend. Dies spart Gerichtskosten und Rechtsverfolgungskosten (vgl. Becker 2015, S. 28).

Maklerklausel

Wird der Versicherungsvertrag über einen Makler (hierzu gehören natürlich auch Inhouse-Broker) abgeschlossen und durch diesen betreut, ist die Aufnahme einer sogenannten Maklerklausel sinnvoll. Diese Klausel regelt, dass alle Anzeigen und Erklärungen, die der Versicherungsnehmer gegenüber dem Versicherer abgibt oder abgeben muss, auch gegenüber dem Makler rechtswirksam abgegeben werden können. Der Versicherungsmakler wiederum übernimmt die Pflicht, diese Informationen an den Versicherer unverzüglich weiterzuleiten.

Klausel zur Rechtswahl/zum Gerichtsstand

Nicht nur international tätige Unternehmen sollten sich überlegen, welcher Gerichtstand und welches nationale Recht im Schadensfall Anwendung findet. Ansonsten können zeitaufwendige Diskussionen über die anwendbaren Rechtsnormen und/oder höhere Rechtsverfolgungskosten entstehen. Einer zügigen Schadenregulierung ist dies nicht zuträglich. Häufig wird daher klarstellend vereinbart, dass für Streitigkeiten bzgl. des Versicherungsvertrages, die sein Zustandekommen, seine Wirksamkeit und die Auslegung von Vertragsklauseln betreffen, ausschließlich deutsches Recht Anwendung findet und (sofern sich der Hauptsitz des Versicherungsnehmers innerhalb Bundesrepublik Deutschland befindet) deutsche Gerichte ausschließlich zuständig sind (vgl. Becker 2015, S. 28).

Klauseln in Verträgen mit All-Risk-Deckungen

Eine besondere Beachtung bei der Vertragsgestaltung verdienen die Verträge mit All-Risk-Deckung. Durch diese Allgefahrendeckung werden alle denkbaren Gefahren, die ursachenunabhängig zu einem Schaden an dem versicherten Risiko führen, versichert. Nicht versicherte Gefahren werden explizit ausgeschlossen. Daher sollte der Versicherungsnehmer ein besonderes Augenmerk auf den Umfang der Ausschlussliste richten. Je weniger Ausschlüsse genannt sind, umso umfangreicher ist der Versicherungsschutz. Probleme bei der Schadenregulierung entstehen, wenn Ausschlüsse nicht klar genug formuliert sind. Unklarheiten sollten bei Vertragsabschluss besprochen und deren gemeinsames Verständnis schriftlich festgehalten werden (zum Beispiel in Form eines side letter).

Repräsentantenklausel

Mit Abschluss des Versicherungsvertrages akzeptiert der Versicherungsnehmer auch verschiedene Obliegenheiten, die er vor, während und nach einem Schadensfall beachten muss. Hält er diese Obliegenheiten nicht ein, kann der Versicherungsanspruch gekürzt werden oder gänzlich entfallen. Es stellt sich daher die Frage, wessen Verhalten für die Erfüllung der Obliegenheiten maßgeblich ist. Klarheit bringt die Repräsentantenklausel. Diese regelt in Abweichung zu § 47 VVG, auf wessen Kenntnis und Verhalten es im Versicherungsfall ankommt. Dabei gilt, dass je weniger natürliche Personen als Repräsentanten des Unternehmens benannt sind, desto niedriger ist die Wahrscheinlichkeit, dass es zu Problemen in der Schadenregulierung aufgrund von verletzten Obliegenheiten kommt (vgl. Becker 2015, S. 29). Als Repräsentanten eines Unternehmens werden häufig die Mitglieder des Vorstandes einer AG, Geschäftsführer einer GmbH, Komplementäre einer KG, Leiter der Rechtsabteilung und Versicherungsabteilung genannt.

Klausel zur Berechnung der Kürzung des Versicherungsanspruchs

Verletzt der Versicherungsnehmer seine vertragliche Obliegenheit grob fahrlässig, ist der Versicherer zur Kürzung des Versicherungsanspruchs in einem der Schwere des Verschuldens entsprechendem Verhältnis berechtigt (§ 28 ff. VVG). Wie die Kürzung angewendet wird, wenn der Versicherungsnehmer mehrere Obliegenheiten verletzt hat, ist durch das Gesetz nicht geregelt. Häufig wendet der Versicherer die Additionsmethode an und der Leistungsanspruch wird auf 0 bis 20 Prozent reduziert (vgl. Becker 2015, S. 29). Um diese für den Versicherungsnehmer ungünstige Situation zu vermeiden, empfiehlt sich die Vereinbarung einer Klausel, die die Additionsmethode ausschließt und stattdessen darauf abstellt, dass bei mehreren Obliegenheitsverletzungen nur die höchste von mehreren gebildeten Kürzungsquoten (jeweils im Verhältnis zur Schwere des Verschuldens des Repräsentanten) zur Anwendung kommt. Bei dieser Gelegenheit sollte in Betracht gezogen werden, die Beweislast für das Vorliegen der groben Fahrlässigkeit auf den Versicherer zu übertragen. Außerdem kann sich der Versicherer trotz Obliegenheitsverletzung auch zur Leistung verpflichten, wenn die Obliegenheitsverletzung weder für den Eintritt bzw. die Feststellung des Schadens noch für die Feststellung bzw. den Umfang der Leistungspflicht ursächlich war.

Klausel zu Rückwirkungsschäden/Wechselwirkungsschäden

Rückwirkungsschäden führen zu Betriebsunterbrechungsschäden, die dadurch entstehen, dass versicherte Sachschäden in Fremdbetrieben (Zulieferer oder Abnehmer) vorliegen. Zum Beispiel kann ein Feuerschaden zu einer Betriebsunterbrechung in einem Fremdbetrieb führen, mit der Folge, dass der Versicherungsnehmer keine Zulieferteile erhält und dadurch ebenfalls eine Betriebsunterbrechung erleidet. Ist der dadurch entstehende Ertragsausfallschaden vom Deckungsschutz umfasst, bedeutet dies für das betroffene Unternehmen eine Erleichterung.

Erfolgen solche Unterbrechungsschäden infolge versicherter Sachschäden in mitversicherten Betrieben innerhalb der eigenen Firmengruppe (Holding, Konzern), sollte ebenfalls der Ertragsausfall versichert sein (sogenannte Wechselwirkungsschäden).

Klausel zu Honorarvereinbarungen mit Rechtsanwälten

In der D&O-Versicherung und in der Rechtsschutz-Versicherung sind die Kosten für die Mandatierung von Rechtsanwälten ein zentraler Bestandteil. Je nach Größe des Schadens sind hoch spezialisierte Rechtsanwälte notwendig, um einen Anspruch abzuwehren, durchzusetzen oder die Verteidigung in einem strafrechtlichen Ermittlungsverfahren wahrzunehmen. Die standardmäßige Kostenübernahme nach der gesetzlichen Gebührenordnung des Rechtsanwaltsvergütungsgesetzes ist hier oft nicht ausreichend, um die notwendige und angemessene Rechtsberatung und Rechtsverteidigung zu gewährleisten. Vielmehr sollte der Deckungsschutz auch Honorarvereinbarungen (in der Regel auf Stundensbasis) mit Rechtsanwälten umfassen. Enthält die Klausel zusätzlich noch die Vereinbarung, dass Stundensätze bis beispielsweise 400 Euro vom Versicherungsschutz gedeckt sind und der Versicherungsnehmer nur bei darüber hinausgehenden Stundensätzen die Einwilligung des Versicherers benötigt, befindet er sich in einer sehr komfortablen Situation. Die Einwilligung des Versicherers zu höheren Stundensätzen bemisst sich dann regelmäßig danach, ob der gewünschte Stundensatz vor dem Hintergrund der Schwierigkeit und Größe des Vorgangs angemessen und notwendig ist. Angaben zur konkreten Höhe des Stundensatzes sind abhängig von der Unternehmensgröße und der Versicherungsparte und müssen individuell festgelegt werden (vgl. Köhns 2018, S. 45).

Klausel zur Erstattung von Allgemeinkosten bei Eigenreparaturen

Häufig entstehen im Zusammenhang mit Eigenreparaturen durch den Versicherungsnehmer Diskussionen darüber, ob Allgemeinkosten vom Versicherer erstattet werden. Unter dem Begriff Allgemeinkosten bezeichnet man Kostenpositionen, die nicht direkt der jeweiligen Reparatur des Schadens zuzuordnen sind (zum Beispiel Verwaltung, Energieversorgung, geleaste Maschinen). Für den Versicherungsnehmer ist die Eigenreparatur oft die sinnvollste Variante, da beauftragte Fremdfirmen die Anlage vor dem Schaden nicht kennen und infolgedessen eine größere Zeitspanne für die Instandsetzung benötigen. Dem Versicherungsnehmer ist daher zu empfehlen, eine gesonderte Klausel einzuführen, wo-

nach er seine Allgemeinkosten (zum Beispiel nach einem prozentualen Anteil in Höhe der aufgewendeten Reparaturkosten) nach durchgeföhrter Eigenreparatur aufschlagen kann (vgl. Becker 2015, S. 30).

Klauseln zu den mitversicherten Kosten

Letztlich sind die mitversicherten Kosten für die Vertragsgestaltung essenziell, da sie neben dem eigentlichen Schaden ebenfalls vom Versicherer ersetzt werden. Unterschieden werden sie in obligatorische und fakultative mitversicherte Kosten.

Nach dem Versicherungsvertragsgesetz hat der Versicherer die obligatorischen (Abwendung und Minderung des Schadens) Kosten zu ersetzen, sie sind also bereits im Deckungsumfang enthalten. Ersetzt werden diese Positionen bis zum Höchstwert, das heißt, Substanz- und Kostenschäden sind auf die Versicherungssumme begrenzt. Fakultative Kosten können mit dem Versicherer individuell (über Klauseln) vereinbart werden. Hierzu zählen unter anderem Aufräumungs-, Abbruch-, Feuerlösch- sowie Bewegungs- und Schutzkosten.

Es empfiehlt sich, die Versicherungssumme in kontinuierlichen Abständen dahingehend zu überprüfen, dass die vereinbarte Versicherungssumme auch die mitversicherten Kosten vollständig im Interesse des Versicherungsnehmers abdeckt.

34.2.4.3 Versicherungssumme

Nach der gesetzlichen Regelung des § 14 VVG ergibt sich für den Versicherer die Pflicht, im Leistungsfall Geldleistungen gegenüber dem Versicherungsnehmer zu erbringen. Die Versicherungssumme begrenzt die Entschädigungsleistung des Versicherers, benennt die höchstmögliche Schadenzahlung an den Versicherungsnehmer in einem Worst-Case-Szenario und ist Basis für die Prämienkalkulation. Der Versicherungsnehmer hat im besten Fall die Qual der Wahl, welche Versicherungssumme für das abzusichernde Risiko angemessen und ausreichend ist. Die Ergebnisse einer aktuellen und fundierten Risikoanalyse des Unternehmens sind für die Entscheidung zur Höhe der Versicherungssumme eine gute Ausgangsbasis. Hieraus können sich weitere Fragen ableiten, wie zum Beispiel:

- Welcher Schutz ist angemessen?
- Was soll überhaupt versichert werden?
- Ist die höchste Versicherungssumme sinnvoll?
- Können Risiken selbst getragen werden? Wenn ja, welche?
- Wie hoch ist die Selbstbeteiligung anzusetzen?

Bei der Wahl der Versicherungssumme ist auf das Zusammenspiel und die Wechselwirkung von Versicherungssumme, Selbstbehalt und Prämie zu achten.

Eine sehr hoch angesetzte Versicherungssumme sorgt zwar für einen ausreichenden Versicherungsschutz in Bezug auf die Erstattung der Schadenshöhe, führt aber unter Um-

ständen zu hohen und dadurch ineffizienten Prämienzahlungen. Im Schadensfall wird der Schaden zwar durch den Versicherer komplett reguliert, fraglich ist aber, ob die dafür entrichtete Prämie noch im Verhältnis steht.

Schäden, die sich im „unteren“ Bereich befinden, können durch einen überschaubaren Selbstbehalt aus der Prämienkalkulation ausgeklammert und damit die Prämie reduziert werden.

Eine zu niedrig angesetzte Versicherungssumme führt hingegen zu Unterversicherung, sodass die Leistungen des Versicherungsnehmers durch den Versicherer gekürzt werden können (es sei denn, es besteht eine Unterversicherungsverzichtsklausel).

Wie im oberen Abschnitt (hier Klausel zu mitversicherten Kosten) erläutert, können ebenfalls zu niedrig angesetzte Versicherungssummen dazu führen, dass die mitversicherten Kosten nicht vollständig ersetzt werden, wenn diese Kosten nicht ausreichend im Rahmen der Ermittlung der Versicherungssumme berücksichtigt worden sind. So hat der Versicherungsnehmer zwar einen Anspruch auf die Versicherungsleistung, eine volle Kostenübernahme durch den Versicherer ist jedoch nicht möglich.

34.2.5 Verantwortlichkeiten und Abläufe

Großschäden, insbesondere Schäden im industriellen Bereich, sind nicht alltäglich. Aufgrund komplexer technischer, wirtschaftlicher und rechtlicher Fragestellungen sowie vielen verschiedenen Beteiligten (vgl. hierzu Abschn. 34.3.1) entstehen häufig Unsicherheiten bzgl. der Vorgehensweise und Regulierung. Dies kann zur Folge haben, dass sich die Bearbeitung des Schadens erheblich verzögert und Mehrkosten für das Unternehmen entstehen. Aus diesem Grund ist es für den Versicherungsnehmer wichtig, ein funktionierendes Schadenmanagement zu etablieren, um während des Schadens handlungsfähig zu sein und seine Obliegenheiten erfüllen zu können.

Ein standardisiertes Verfahren ist bei Großschäden selten möglich. Umso wichtiger ist es, dass in solch einem Fall alle Bearbeitungsprozesse ineinander greifen und die betroffenen Abteilungen und Unternehmensbereiche eng zusammenarbeiten. Die Basis für eine effiziente Abwicklung mit dem Versicherungsunternehmen bilden strukturierte Prozesse, Kontrollmechanismen, festgelegte Verantwortlichkeiten sowie klare Kommunikationskanäle mit allen Unternehmensabteilungen (vgl. Neumeister 2015, S. 8).

Bei der Zuordnung der Verantwortlichkeiten auf der Unternehmensseite empfiehlt sich, dass die betroffenen Personen mit der Infrastruktur sowie den Prozessen gut vertraut sind. Kompetenzen sollten innerhalb dieses Kreises klar abgegrenzt werden, wenngleich der Blick über den eigenen „Kompetenztellerrand“ regelmäßig hilfreich sein kann, um in Sonderkonstellationen genügend Raum für notwendige individuelle Entscheidungen zu haben. In Zusammenarbeit mit dem Versicherer kann vereinbart werden, welcher Schadenregulierer und Sachverständige im Schadenfall mit der Regulierung betraut wird. Zusätzlich sollten die Tätigkeitsbereiche der beiden Parteien klar festgelegt werden.

Die Abläufe können für die Bearbeitung durch das eigene Schadenmanagement in drei Phasen dargestellt werden (in Anlehnung an Neumeister 2015, S. 8 bis 9):

Phase 1 – Interne Schadenbearbeitung

Diese Phase umfasst die Sammlung und Dokumentation der sachlichen Informationen zum Schadenshergang, zur Schadenshöhe und zur Beweissicherung sowie die Prüfung des Versicherungsschutzes. Diese Vorarbeit ermöglicht eine effizientere Bearbeitung des Schadens sowohl für den Versicherungsnehmer als auch für den Versicherer. Parallel erfolgen eine Anzeige des Schadens beim Versicherer und die Übermittlung aller Daten und Informationen zum Schadenvorgang.

Phase 2 – Interaktion mit dem Versicherer

Liegen alle Informationen vor, kann die ggf. notwendige Schadenbesichtigung durch das Versicherungsunternehmen vorbereitet und durchgeführt werden. Nach der Besichtigung zeigt sich, ob beide Parteien die gleiche Sichtweise auf den Sachverhalt haben oder ob noch weiterer Klärungsbedarf besteht. Letzterer entsteht häufig durch unterschiedliche Interpretationen der Versicherungsbedingungen und kann durch klar formulierte Klauseln vermieden werden. Erkennt der Versicherer den Schadensfall dem Grunde nach an, kann zum Beispiel eine Abschlagszahlung vereinbart werden. Weitere Schritte in der Regulierung sind eng abzustimmen, um Missverständnisse zu vermeiden. Die Vereinbarung von regelmäßigen Terminen mit dem Versicherer, um den aktuellen Sachstand zu besprechen, ist eine gute Basis für eine für beide Seiten zufriedenstellende Regulierung.

Phase 3 – Schadencontrolling

Nach der Regulierung des Schadens durch den Versicherer erfolgt die interne Evaluation. Bei diesem Schritt werden die internen Prozesse sowie die Abläufe beim Schaden kritisch hinterfragt und reflektiert. Das Schadencontrolling wird detailliert im Abschn. 34.4.1 behandelt.

Neben der Festlegung von Verantwortlichkeiten und Abläufen kann die Erstellung eines Notfallplans bzw. eines Notfallhandbuchs für den Schadensfall sinnvoll sein. Dabei werden die genaue Vorgehensweise und Abläufe im Schadensfall für alle beteiligten Personen dokumentiert und beschrieben. Dies kann auch in Zusammenarbeit mit einem Versicherer und/oder Makler entstehen. Zusätzliche Inhalte können zum Beispiel ein Krisenmanagementplan, unternehmenseigene Ablaufpläne, ein Business-Recovery-Plan, Adress- und Checklisten sein.

Der beste Notfallplan kann jedoch in einem Ernstfall versagen, sofern er nicht regelmäßig aktualisiert und anhand von Probe-Schadensfällen simuliert wird. Korrekturen von Produktionsprozessen, modernisierte Maschinen und Anlagen wie auch wechselndes Personal sind Beispiele, die zu einer notwendigen Überarbeitung des Notfallplanes führen können. Damit ein einheitlicher aktueller Stand über diese Neuerungen für alle Mitarbeiter zur Verfügung steht, sind regelmäßige Schulungen und Seminare unabdingbar.

34.3 Während des Schadens

34.3.1 Beteiligte im Schadensprozess

Innerhalb eines Regulierungs- bzw. Schadensprozess sind unterschiedliche Parteien beteiligt (vgl. Abb. 34.3). In diesem Abschnitt werden die wichtigsten Stakeholder und deren Funktionen bzw. Aufgaben während des Schadens kurz erläutert.

Versicherungsnehmer

In einem Schadensfall steht der Versicherungsnehmer im Zentrum des Regulierungsprozesses. Je nach Fall kann er als Geschädigter (zum Beispiel Feuerschaden in einer Betriebsstätte) oder Schädiger (zum Beispiel Dritte werden im Rahmen eines Unfalls verletzt) auftreten. Zu seinen (Pflicht)-Aufgaben im Schadensfall gehören die Meldung, Abwendung, Minderung und Dokumentation des Schadens sowie die Anwendung des internen Notfallplans (sofern vorhanden).



Abb. 34.3 Beteiligte im Regulierungs- bzw. Schadenprozess. (Quelle: eigene Darstellung)

Versicherungsmakler/Inhouse-Broker

Haupthaufgabe des Maklers/Inhouse-Brokers ist im Schadenfall die zielgerichtete Abwicklung und Kommunikation mit dem Versicherer. Dazu gehört die Entgegennahme der Schadenmeldung vom Versicherungsnehmer, die Sammlung und Aufbereitung aller relevanten Daten und Informationen, sodass diese zeitnah gebündelt an den Versicherer zur weiteren Bearbeitung gesendet werden können. Der Makler/Inhouse-Broker koordiniert, strukturiert und stimmt die weiteren Schritte mit dem Versicherungsnehmer und dem Versicherer ab.

Versicherer/Schadenregulierer

Neben der klassischen Schadenregulierung durch den Versicherer werden bei Großschäden oft spezialisierte Schadenregulierer eingesetzt, um den Schaden seitens des Versicherers zu koordinieren und vollständig abzuwickeln. Sie führen die Erstbesichtigung der Schadenstelle durch und vergeben Aufträge, zum Beispiel an Sachverständige und Sanierungsunternehmen. Zudem stehen sie idealerweise in ständigem Kontakt zum Versicherungsnehmer/Versicherungsmakler, um die nächsten Schritte vorzubereiten.

Sachverständige

Ein Sachverständiger erarbeitet die technischen Sachverhalte eines Schadens. Bei einem Einsatz von Sachverständigen hat der Versicherungsnehmer die Wahlmöglichkeit, ob er das Beiratsverfahren oder das Sachverständigenverfahren wünscht. In der ersten Variante ermittelt der Sachverständige für beide Parteien den Sachverhalt. Beim Sachverständigenverfahren beauftragen sowohl der Versicherungsnehmer als auch der Versicherer jeweils einen Sachverständigen, mit dem Ziel, sich nach Abschluss der Gutachtentätigkeiten auf ein Ergebnis zu einigen. Ist eine Einigung nicht möglich, erfolgt die Einschaltung eines dritten Sachverständigen, der als Obmann agiert. Beide Varianten weisen Vor- und Nachteile auf, deren Bewertung einzelfallabhängig ist. In der Praxis zeigt sich die Tendenz, dass je komplexer oder größer ein Schadenfall ist, Versicherer und Versicherungsnehmer bevorzugt einen eigenen Sachverständigen beauftragen. Es sollte dabei auf eine reibungslose Zusammenarbeit zwischen den Sachverständigen geachtet werden, damit eine Abwicklung nicht aus fachlichen oder emotionalen Gründen zusätzlich erschwert wird (vgl. Hergarten 2018, S. 6 bis 7).

Sanierungsunternehmen

Diese Betriebe haben sich darauf spezialisiert, die nach einem Schaden betroffenen Gebäude, Maschinen und Anlagen zu trocknen und zu reinigen. Die „Sanierer“ gehören zu den ersten „Besuchern“ der Schadenstätte und verfügen aufgrund ihres Geschäftsmodells über gute Kontakte zur Versicherungsbranche (vgl. Jacobs 2018, S. 5). Beauftragt werden diese Unternehmen in der Regel durch den Versicherer.

Rechtsanwälte

Rechtsanwälte helfen dabei, unberechtigte Schadensersatzansprüche gegenüber dem Versicherungsnehmer abzuwehren, setzen Deckungsansprüche gegenüber dem Versicherer durch oder übernehmen die Verteidigung bzw. Rechtsberatung der versicherten Person.

Behörden

Verschiedenste Behörden können neben den klassischen Schadensparteien in einem Schadensfall beteiligt sein. Liegen Personenschäden vor, kann das staatliche Amt für Arbeitsschutz (bzw. die jeweilige Landesbehörde oder Bezirksregierung) von Amts wegen involviert sein. Aber auch Umweltämter, Baubehörden oder Gewerbeaufsichtsämter sind potenziell Beteiligte im Schadensprozess. Informationen und Unterlagen, die von den Behörden angefordert werden, sollten nur durch autorisierte Personen des Unternehmens bearbeitet werden. So kann sichergestellt werden, dass keine Informationslücken mit unkalkulierbaren Folgen entstehen (vgl. Hergarten 2018, S. 7).

IT-Spezialisten

Bei Cybersicherheitsvorfällen sollte ein IT-Spezialist hinzugezogen werden. Diese Partei sorgt mithilfe von IT-Forensik nach einem Angriff bzw. Vorfall für die Wiederherstellung notwendiger Daten und die Aufdeckung der Sicherheitslücken. In diesem Prozess können sowohl interne als auch externe Berater involviert sein.

Öffentlichkeit

Die Öffentlichkeit (zum Beispiel Presse, Nachbarschaft) ist eine besonders sensible Interessengruppe, deren indirekter Einfluss auf die Schadenregulierung nicht zu unterschätzen ist. Dabei ist es ratsam, eine Person oder ein Team zu betrauen, welche/s über ausreichend Erfahrung und das notwendige Know how im Umgang mit der Presse- und Öffentlichkeitsarbeit in Krisen- und Schadenssituationen besitzt.

34.3.2 Erste Schritte

Der erste Schritt im Schadenfall ist die Schadensmeldung. Abhängig vom Schaden, sollte diese mindestens folgende Punkte umfassen:

- Versicherungsnehmer
- Versicherungsnummer
- Schadentag
- Schadenort
- Schadenursache/-hergang
- voraussichtliche Schadenhöhe (grobe Schätzung)
- Bilder des Schadens (sofern vorhanden).

34.3.2.1 Koordination

Die Schadenkoordination soll sicherstellen, dass ein reibungsloser und zügiger Regulierungsprozess gewährleistet wird und unnötige bzw. fehlerhafte Regulierungsschritte vermieden werden. Um dies zu ermöglichen, sind Kommunikationsrichtlinien festzulegen, damit die beauftragten Personen stets den Gesamtüberblick sowie die Kontrolle behalten. Im Zentrum steht die Informations- und Aufgabenweitergabe an die einzelnen Bereiche und Ebenen (vgl. Abschn. 34.2.5).

34.3.2.2 Schadenminderungsmaßnahmen

Die Maßnahmen zur Schadenbegrenzung und -minderung fallen in der Regel dem Versicherungsnehmer zu. Dabei hat das versicherungsnehmende Unternehmen die Weisungen des Versicherers (soweit zumutbar) einzuhören und zu befolgen. Die entstandenen Kosten werden vom Versicherer ersetzt. Die gesetzlichen Regelungen befinden sich in den §§ 82, 83 sowie 90 VVG.

Diese Maßnahmen verhindern bzw. minimieren Folgekosten durch weitere Schäden und liegen damit im Interesse von Versicherer und Versicherungsnehmer (vgl. Abb. 34.4).

Sofortmaßnahmen

Der Zeitfaktor spielt in der Schadenregulierung eine wesentliche Rolle. Ein reibungsloser, unbürokratischer und schneller Ablauf der Schadenregulierung kann für das betroffene Unternehmen existenzentscheidend sein. Zum Beispiel sind in der Sachversicherung bei Großschäden sogenannte Akontozahlungen (Abschlagszahlungen) als Soforthilfe für Erstmaßnahmen im Einzelfall unverzichtbar. Denn das geschädigte Unternehmen wird, wegen des Bestehens einer Versicherung, keine eigenen Rückstellungen für den Eintritt des verwirklichten Risikos gebildet haben (Münchner Kommentar VVG § 14, Rdn. 16; vgl.

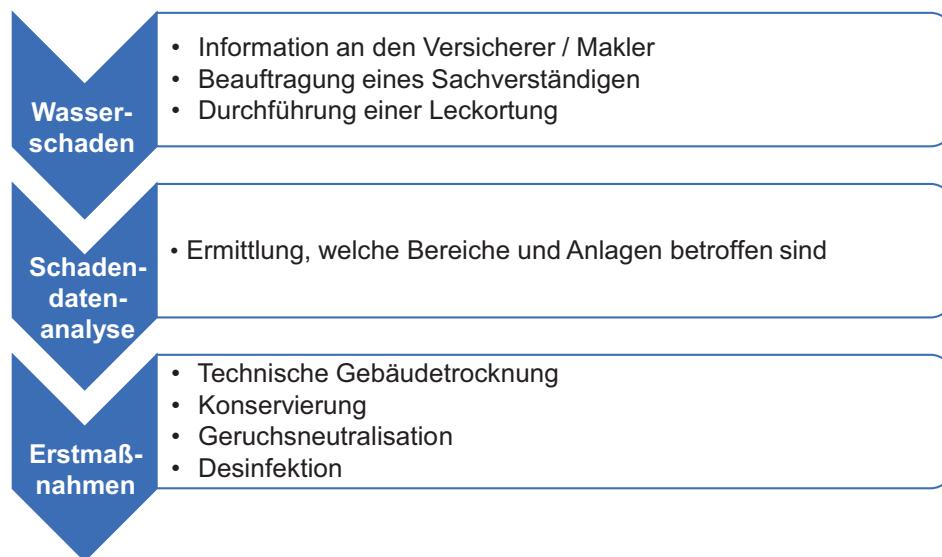


Abb. 34.4 Schadenminderung – mögliche Schritte am Beispiel eines Wasserschadens. (Quelle: eigene Darstellung in Anlehnung an Robold et al. 2017, S. 151)

Munkwitz 2015, S. 6). Diese schnelle Soforthilfe liegt ebenfalls im Interesse des Versicherers, der dadurch einen aus dem Schaden folgenden Betriebsunterbrechungsschaden geringhalten kann (Produktion an einem Ausweichstandort, Anmietung einer identischen Anlage). Weitere Sofortmaßnahmen könnten sein:

- Absicherung von Schadenstellen, die ein unbefugtes Betreten verhindern
- unverzügliche Trennung betroffener Anlagen und Maschinen von der Stromversorgung
- Absicherung gegen Witterungseinflüsse
- Durchlüften der vom Schaden betroffenen Räume
- Sicherung der IT-Standorte sowie der Datenträger.

Es kommt jedoch nicht nur auf eine Ad-hoc-Reaktion bei der Schadenminderung an. Die Sofortmaßnahmen sind so zu planen und zu steuern, dass die Arbeiten effizient aufeinander abgestimmt sind.

34.3.3 Krisenkommunikation

Bei einem Großschaden, der sich zu einem Krisenfall entwickelt, ist der Wert einer guten Krisenkommunikation in Zeiten von Facebook, Twitter und anderer sozialer Medien im Hinblick auf die Reputation des Unternehmens nicht zu unterschätzen. Auch die Schadensbeteiligten werden in ihren Einstellungen und Handlungen durch die Krisenkommunikation – bewusst oder unbewusst – beeinflusst.

Innerhalb der Krisenkommunikation stellt es eine besondere Herausforderung dar, die vielen verschiedenen Informationen zusammenzufassen, der Öffentlichkeit die notwendigen Informationen mitzuteilen und Verantwortung zu zeigen. Erste Schritte können sein:

- Inbetriebnahme einer Hotline für Kunden, Geschädigte etc.
- Beauftragung einer externen PR-Agentur (wenn keine unternehmenseigene PR-Abteilung vorhanden oder zur Unterstützung)
- aktives Nutzen sozialer Medien (neben den klassischen Medien wie Fernsehen, Zeitung und Radio) zur Steuerung der Krisenkommunikation
- Aufstellen von Kommunikationsregeln für Mitarbeiter und Unternehmensleitung, um einheitliche und widerspruchsfreie Informationen gegenüber der Öffentlichkeit zu gewährleisten
- Erstellung eines Fragen- und Antwortkatalogs einschließlich dessen laufende Aktualisierung
- Dokumentation von Statusreports und Aktionsplänen für die Kommunikation (vgl. Barth et al. 2016, S. 24 bis 25).

34.3.4 Obliegenheiten im Schadensfall

Im Schadensfall hat der Versicherungsnehmer gesetzliche und vertragliche Regelungen einzuhalten, um seinen Versicherungsanspruch nicht zu gefährden. Diese Obliegenheiten, wie zum Beispiel Anzeige-, Auskunfts- und Mitwirkungspflichten, treffen nicht nur den Versicherungsnehmer, sondern auch mitversicherte Gesellschaften.

Für die Anzeigepflicht gilt, dass dem Versicherer der Schadensfall form- und fristgerecht angezeigt werden muss. Sollte das jeweilige Risiko von mehreren Versicherern getragen werden und keine Führungsklausel vereinbart worden sein, muss der Versicherungsfall jedem einzelnen Versicherer angezeigt werden.

Damit der Versicherer den Schaden schnell regulieren kann, werden verschiedene Informationen für ein umfassendes Schadensbild angefordert. Auch hier wird deutlich, dass eine Organisationsstruktur beim Versicherungsnehmer, die eine sorgfältige und umfangreiche Dokumentation von Schadensfällen sicherstellt, die Erfüllung der Auskunftspflicht wesentlich erleichtert.

Dass der Versicherungsnehmer im Rahmen der Schadenregulierung mit dem Versicherer kooperieren (Mitwirkungsobliegenheit) und den Weisungen des Versicherers zur Schadensabweitung bzw. -minderung nachkommen sollte, versteht sich von selbst. Zu diesen Mitwirkungsobliegenheiten zählt auch, dass ohne vorherige Absprache mit dem Versicherer keine Zugeständnisse gegenüber dem Geschädigten gemacht werden sollten. Aus geschäftspolitischen Gründen mag es sinnvoll sein, den geschädigten Kunden bzw. Geschäftspartner in den ersten Momenten eines Schadens durch Spontanzusagen emotional abzuholen, im Hinblick auf eine sinnvolle und erfolgreiche Schadenregulierung ist dies eher kontraproduktiv. Aus diesem Grund ist ein funktionierendes internes Risiko- bzw. Schadenmanagement entscheidend, damit alle Obliegenheiten erfüllt werden (vgl. Drave 2015, S. 24 ff.).

34.4 Nach dem Schaden

34.4.1 Schadencontrolling

Ist die Schadenhöhe geprüft, durch den Versicherer frei gegeben und reguliert, erfolgt die Evaluation des gesamten Schadenprozesses. Getreu dem Motto „Aus Schaden wird man klug“ sind in dieser Phase alle internen Prozesse und Abläufe während des Schadens kritisch zu betrachten, zu reflektieren und ggf. zu optimieren. Zusätzlich kann das Schadencontrolling nach einem Schaden, außerhalb der regelmäßigen Prüfung des Versicherungsvertrages, dazu beitragen, zusammen mit dem Makler bzw. Versicherer Deckungslücken zu erkennen und zu schließen. Auch dafür ist Voraussetzung, dass saubere Nachweise in den jeweiligen Bearbeitungsschritten des eigenen Schadenmanagements (im besten Fall per Knopfdruck) vorliegen, um dieses Controlling durchführen zu können (vgl. Neumeister 2015, S. 9).

Neben der Überprüfung der eigenen Prozesse und Abläufe sollte auch die Zusammenarbeit mit dem Versicherungsmakler und Versicherer betrachtet werden. Faktoren wie Bearbeitungsdauer, Kompetenz, vorausschauende Koordination, Erreichbarkeit, Termintreue, serviceorientierte Korrespondenz und das Regulierungsverhalten des Versicherers sind Eigenschaften und Merkmale, die in die Bewertung einfließen. Eine unprofessionelle Schadenregulierung ist genauso rufschädigend für ein Unternehmen, wie ein unnachgiebi-

ges und kasuistisches Verhalten im Falle von Schadenersatzansprüchen Dritter. Ein ausgewogenes Verhältnis zwischen dem Erledigungs- und wirtschaftlichem Eigeninteresse des Versicherers, dem Interesse des Versicherungsnehmers am Fortbestand seiner Geschäftsbeziehungen und seines Unternehmens respektive seiner Reputation und dem Schutz der Versicherungssolidargemeinschaft ist dabei essenziell. Entweder bestätigt sich die erfolgreiche Zusammenarbeit, muss optimiert oder beendet werden. Wie das Ergebnis auch ausfällt, das Schadencontrolling sollte nicht vernachlässigt werden, denn bekanntermaßen ist „Nach dem Schaden vor dem Schaden“.

34.4.2 Reputation

Unternehmen, die einen Großschaden erlitten und entsprechende Medienaufmerksamkeit erhalten haben, stehen in den Augen der Öffentlichkeit erst einmal „unter Beobachtung“. Insbesondere bei Schäden, die die Öffentlichkeit erreichen (zum Beispiel Datenschutz, Großbrand, Chemieunfall), ist eine Kommunikation nach außen wichtig, die aufzeigt, dass Schwachstellen erkannt und zusätzliche Sicherheitsmaßnahmen eingeleitet wurden. Durch Maßnahmen, wie die Einbindung von Spezialisten, Veröffentlichungen in Fachzeitschriften, Diskussionsbeiträge in der Öffentlichkeit und Investitionen in verbesserte Technik, kann das Unternehmen aktiv dazu beitragen, Reputationsschäden nachhaltig zu beseitigen (vgl. Barth et al. 2016, S. 26 bis 27).

Außerdem können Unternehmen bei Bedarf spezielle Versicherungen abschließen, die Reputationsschäden abdecken. Die Produkte variieren je nach Versicherer stark, da es sich um individuelle Versicherungen handelt, welche mit verschiedenen Ansätzen und unterschiedlichen Reichweiten entwickelt wurden (vgl. Klinkhammer 2016, S. 4).

34.5 Ausblick

Durch den stetigen Wandel und die Digitalisierung kann die Schadenregulierung in Zukunft um ein Vielfaches schneller und automatischer geschehen, als noch vor einigen Jahren. Anhand sogenannter smart contracts wird es in naher Zukunft möglich sein, Verträge als Programmcode abzubilden. Vorher eingegebene Sensoren erfassen den Schadensfall und per Schnittstelle werden automatisierte Rechtsfolgen ausgelöst. Beispielsweise messen Sensoren in Industrieanlagen die Wetterlage und übertragen die Messdaten an eine Datenbank, so dass hiermit Wasserschäden automatisch gemeldet werden können. Bei Überschreitung vorher festgelegter Messwerte werden automatisiert Schadenzahlungen (Pauschale) durch die smart contracts an den Versicherungsnehmer angewiesen sowie Gutachter und Sanierungsunternehmen informiert. Dadurch ist es möglich, Schäden direkt zu begrenzen bzw. zu mindern, schneller in die Regulierung einzutreten und dem Versicherungsnehmer direkt mit berechtigten Schadensansprüchen entgegen zu kommen (vgl.

Möhlenkamp und Wessel 2018, S. 34 ff.). Denkbar ist die Anwendung dieser Technologie ebenfalls in der Transportversicherung. Durch Live-Tracking der Fahrzeuge können Standort, Zustand der Ware und Temperatur übermittelt und in einem Notfall direkt adäquate Maßnahmen eingeleitet werden.

Im Rahmen von Großschäden wird es anhand von intelligenter Bilderkennung zukünftig möglich sein, durch Satellitenbilder und Luftaufnahmen präzise Informationen über die Entstehung von Schäden zu erhalten. Dies ermöglicht es, den Einsatz von Gutachtern und Vor-Ort-Besichtigungen effizient zu gestalten und schnell in eine Regulierung überzugehen (vgl. Schadentopics – Zukunft des Schadenmanagements 2017, S. 5).

Literatur

- Barth, M., et al. (2016). Kosten eines Cyberfalls: Leitfaden. https://www.hisolutions.com/fileadmin/user_upload/Infocenter/SecCon/Leitfaden_Bitkom_Kosten_Cyber-Schadensfall.pdf. Zugegriffen am 26.06.2019.
- Becker, C. (2015). Reibungslose Schadenregulierung durch vorausschauende Vertragsklauseln. *Die VersicherungsPraxis*, 4/2015, 28–30.
- Drave, C. (2015). Grossschäden – Herausforderungen bei der Schadenregulierung. *Die VersicherungsPraxis*, 1/2015, 24–27.
- Hergarten, T. (2018). Serviceorientiertes Schadenmanagement – Erwartungen an den Versicherungsmakler bei Gross- oder Komplexschäden. *Die VersicherungsPraxis*, 2/2018, 6–8.
- Hochwasser – Risiken für Unternehmen. (2016). Hrsg. Ministerium für Umwelt, Klima und Energiewirtschaft Baden-Württemberg. https://www.hochwasser.baden-wuerttemberg.de/documents/43970/44031/Risiken_fuer_Unternehmen.pdf/1de8d296-2fe2-428f-8914-d657070d062a. Zugegriffen am 26.06.2019.
- Jacobs, K. (2018). Die Abwicklung von Großschäden in der Praxis – Ein Soll-Ist-Abgleich. *Schadenpraxis*, 01/2018, 4–9.
- Klinkhammer, G. (2016). Reputationsverlust und die Folgen – Aktuelle Versicherungsmöglichkeiten für Unternehmen. *Die VersicherungsPraxis*, 3/2016, 14–15.
- Köhns, O. (2018). Der D&O Schadenfall in der Praxis. *Die Versicherungspraxis*, 10/2018, 44–45.
- Möhlenkamp, M., & Wessel, T. (2018). Smart Contracts in der Versicherung – Chancen und Rechtliche Herausforderungen. *Die VersicherungsPraxis*, 05/2018, 34–37.
- Munkwitz, B. (2015). Schadenregulierung. *Die VersicherungsPraxis*, 04/2015, 3–7.
- Neumeister, V. (2015). Mehrwert für das Unternehmen durch professionelles Schadenmanagement. *Die VersicherungsPraxis*, 04/2015, 8–9.
- Robold, M. O., Schmitz, S., & Berthold, C. (2017). *Schaden- und Leistungsmanagement: Sachversicherungen für private und gewerbliche Kunden* (2. Aufl.). Karlsruhe: Versicherungswirtschaft GmbH.
- Rohlf, T. (2018). *Risikomanagement im Versicherungsunternehmen: Identifizierung, Bewertung und Steuerung*. Karlsruhe: Versicherungswirtschaft GmbH.
- Rüffer, W., et al. (2015). *Versicherungsvertragsgesetz* (3. Aufl., Dr. W. Rüffer, Dr. D. Halbach, Prof. Dr. P. Schimikowski, Hrsg.). Baden-Baden: Nomos.
- Schadentopics: Zukunft des Schadenmanagements. (2017). Hrsg. Munich Re. https://www.munichre.com/site/touch-publications/get/documents_E-1609853527/mr/assetpool.shared/Documents/5_Touch/_Publications/09051_SSP_2017_de.pdf. Zugegriffen am 24.06.2019.

Birgit Beudt studierte Rechtswissenschaften an der Universität Leipzig / Frankfurt am Main und arbeitete zunächst als Rechtsanwältin in den Bereichen des Sozial-, Kranken- und Rentenversicherungsrechts. Von 2011 bis 2019 war sie beim Inhouse Broker der Fraport AG und deren Beteiligungen unter anderem verantwortlich für die Analyse, Beratung und Platzierung von Directors & Officers-Versicherungen mit internationalen Lokalpolicen, Vertrauensschaden-, Rechtsschutz- und Verkehrshaftungsversicherungen sowie für die diesbezügliche Koordination und Begleitung von Schadensfällen. Seit dem 01.01.2020 ist Frau Beudt als Rechtsanwältin und Syndikusrechtsanwältin bei der VSW - Die Versicherergemeinschaft für Steuerberater und Wirtschaftsprüfer mit allen rechtlichen Fragestellungen im Zusammenhang mit der Gewähr und der Gestaltung von Berufshaftpflichtversicherungen für Steuerberater, Wirtschaftsprüfer und deren Berufsträgergesellschaften tätig. Bereits in ihrer Publikation in „Die VersicherungsPraxis“, 04/2015, 3-7 hat Frau Beudt (geb. Munkwitz) sich dem Thema der Schadenregulierung gewidmet. Der Artikel wurde auch in der Bibliothek des BGH aufgenommen (neue Aufsätze 4.5 - 8.5.2015).

Frank Cremer studierte Versicherungswesen mit den Schwerpunkten Rückversicherung, Bilanzierung von Versicherungsunternehmen und Sachversicherung am Institut für Versicherungswesen der Technischen Hochschule Köln. Im Anschluss absolvierte er dort auch das Masterstudium Risk & Insurance. Neben dem Studium hat er internationale Studierende unterstützt und engagiert sich als Wissenschaftlicher Mitarbeiter an der Kölner Forschungsstelle für Rückversicherung und erwarb den Titel des Fellow of the Chartered Insurance Institute in London (FCII).