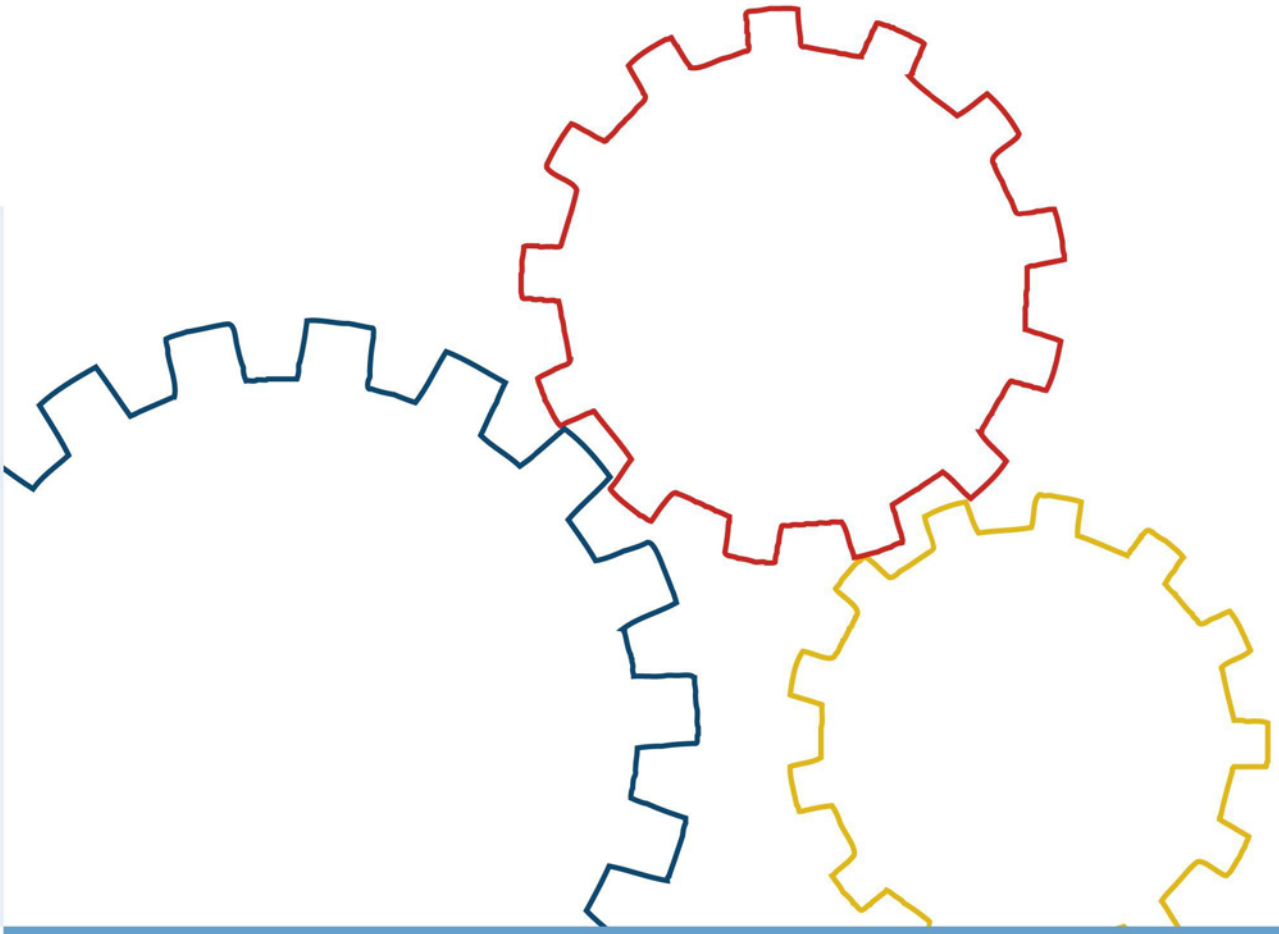
Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Standard 200-3

Risikoanalyse auf der Basis von IT-Grundschutz



www.bsi.bund.de/grundschutz

Version 1.0

BSI-Standard 200-3

Risikoanalyse auf der Basis von IT-Grundschutz

Version 1.0, Oktober 2017

Inhaltsverzeichnis

1 Einleitung

1.1 Versionshistorie

Der BSI-Standard 200-3 löst den BSI-Standard 100-3 ab.

Stand	Version	Änderungen
Oktober 2016	CD 1.0	Neukonzeption basierend auf BSI-Standard 100-3 • Risikoanalyse auf die elementaren Gefährdungen umgestellt • Einführung Matrix-Ansatz zur Bewertung von Risiken • Einführung Risikoappetit und Chancenmanagement
Oktober 2017	1.0	Einarbeitung Anwenderkommentare • Begriffe "Eintrittswahrscheinlichkeit" und "Handlungsalternativen" durch "Eintrittshäufigkeit" bzw. "Handlungsoptionen" ersetzt • Gegenüberstellung von Begriffen aus ISO/IEC 31000 und dem BSI-Standard 200-3 • Kapitel Risikoeinstufung unterteilt in Risikoeinschätzung und Risikobewertung • Scope des Dokuments auf die Darstellung der Risikoanalyse konzentriert • Glossar überarbeitet

1.2 Zielsetzung

Mit dem BSI-Standard 200-3 stellt das BSI ein leicht anzuwendendes und anerkanntes Vorgehen zur Verfügung, mit dem Institutionen ihre Informationssicherheitsrisiken angemessen und zielgerichtet steuern können. Das Vorgehen basiert auf den elementaren Gefährdungen, die im IT-Grundschutz-Kompendium beschrieben sind und auf deren Basis auch die IT-Grundschutz-Bausteine erstellt werden.

In der Vorgehensweise nach IT-Grundschutz wird bei der Erstellung der IT-Grundschutz-Bausteine implizit eine Risikobewertung für Bereiche mit normalem Schutzbedarf vom BSI durchgeführt. Hierbei werden nur solche Gefährdungen betrachtet, die eine so hohe Eintrittshäufigkeit oder so einschneidende Auswirkungen haben, dass Sicherheitsmaßnahmen ergriffen werden müssen. Typische Gefährdungen, gegen die sich jeder schützen muss, sind z. B. Schäden durch Feuer, Wasser, Einbrecher, Schadsoftware oder Hardware-Defekte. Dieser Ansatz hat den Vorteil, dass Anwender des IT-Grundschutzes für einen Großteil des Informationsverbundes keine individuelle Bedrohungs- und Schwachstellenanalyse durchführen müssen, weil diese vorab vom BSI bereits durchgeführt wurde.

In bestimmten Fällen muss jedoch explizit eine Risikoanalyse durchgeführt werden, beispielsweise wenn der betrachtete Informationsverbund Zielobjekte enthält, die

- einen hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit haben oder
- mit den existierenden Bausteinen des IT-Grundschutzes nicht hinreichend abgebildet (modelliert) werden können oder

- in Einsatzszenarien (Umgebung, Anwendung) betrieben werden, die im Rahmen des IT-Grundschutzes nicht vorgesehen sind.

In diesen Fällen stellen sich folgende Fragen:

- Welchen Gefährdungen für Informationen ist durch die Umsetzung der relevanten IT-Grundschutz-Bausteine noch nicht ausreichend oder sogar noch gar nicht Rechnung getragen?
- Müssen eventuell ergänzende Sicherheitsmaßnahmen, die über das IT-Grundschutz-Modell hinausgehen, eingeplant und umgesetzt werden?

Das vorliegende Dokument beschreibt, wie für bestimmte Zielobjekte festgestellt werden kann, ob und in welcher Hinsicht über den IT-Grundschutz hinaus Handlungsbedarf besteht, um Informationssicherheitsrisiken zu reduzieren. Hierzu werden Risiken, die von elementaren Gefährdungen ausgehen, eingeschätzt und anhand einer Matrix bewertet. Die Einschätzung erfolgt über die zu erwartende Häufigkeit des Eintretens und die Höhe des Schadens, der bei Eintritt des Schadensereignisses entsteht. Aus diesen beiden Anteilen ergibt sich das Risiko.

Im vorliegenden BSI-Standard 200-3 ist die Risikoanalyse zweistufig angelegt. In einem ersten Schritt wird die in Kapitel 4 erstellte Gefährdungsübersicht systematisch abgearbeitet. Dabei wird für jedes Zielobjekt und jede Gefährdung eine Bewertung unter der Annahme vorgenommen, dass bereits Sicherheitsmaßnahmen umgesetzt oder geplant worden sind (siehe Beispiele in Kapitel 5). In der Regel wird es sich hierbei um Sicherheitsmaßnahmen handeln, die aus den Basis- und Standard-Anforderungen des IT-Grundschutz-Kompendiums abgeleitet worden sind. An die erste Bewertung schließt sich eine erneute Bewertung an, bei der Sicherheitsmaßnahmen zur Risikobehandlung betrachtet werden (siehe Beispiele in Kapitel 6). Durch einen Vorher-Nachher-Vergleich lässt sich die Wirksamkeit der Sicherheitsmaßnahmen prüfen, die zur Risikobehandlung eingesetzt worden sind.

1.3 Abgrenzung, Begriffe und Einordnung in den IT-Grundschutz

Chancen und Risiken sind die häufig auf Berechnungen beruhenden Vorhersagen eines möglichen Nutzens im positiven Fall bzw. Schadens im negativen Fall. Was als Nutzen oder Schaden aufgefasst wird, hängt von den Wertvorstellungen einer Institution ab.

Dieser Standard konzentriert sich auf die Betrachtung der negativen Auswirkungen von Risiken, mit dem Ziel, adäquate Maßnahmen zur Risikominimierung aufzuzeigen. In der Praxis werden im Rahmen des Risikomanagements meistens nur die negativen Auswirkungen betrachtet. Ergänzend hierzu sollten sich Institutionen jedoch durchaus auch mit den positiven Auswirkungen befassen.

Risikoanalyse

Als Risikoanalyse wird in diesem Werk der komplette Prozess bezeichnet, um Risiken zu beurteilen (identifizieren, einschätzen und bewerten) sowie zu behandeln. Risikoanalyse bezeichnet aber nach den einschlägigen ISO-Normen ISO 31000 (siehe [31000]) und ISO 27005 (siehe [27005]) nur einen Schritt im Rahmen der Risikobeurteilung, die aus den folgenden Schritten besteht:

- Identifikation von Risiken (Risk Identification)
- Analyse von Risiken (Risk Analysis)
- Evaluation oder Bewertung von Risiken (Risk Evaluation)

Im deutschen Sprachgebrauch hat sich allerdings der Begriff Risikoanalyse für den kompletten Prozess der Risikobeurteilung und Risikobehandlung etabliert. Daher wird im IT-Grundschutz und auch in diesem Dokument weiter der Begriff Risikoanalyse für den umfassenden Prozess benutzt.

Die Risikoanalyse nach BSI-Standard 200-3 sieht folgende Schritte vor (siehe auch Abbildung 1), die in den jeweiligen Kapiteln ausführlicher betrachtet werden.

- Schritt 1: Erstellung einer Gefährdungsübersicht (siehe Kapitel 4)
    - Zusammenstellung einer Liste von möglichen elementaren Gefährdungen

  - Ermittlung zusätzlicher Gefährdungen, die über die elementaren Gefährdungen hinausgehen und sich aus dem spezifischen Einsatzszenario ergeben

- Schritt 2: Risikoeinstufung (siehe Kapitel 5)
  - Risikoeinschätzung (Ermittlung von Eintrittshäufigkeit und Schadenhöhe)
  - Risikobewertung (Ermittlung der Risikokategorie)
- Schritt 3: Risikobehandlung (siehe Kapitel 6)
  - Risikovermeidung
  - Risikoreduktion (Ermittlung von Sicherheitsmaßnahmen)
  - Risikotransfer
  - Risikoakzeptanz
- Schritt 4: Konsolidierung des Sicherheitskonzepts (siehe Kapitel 7)
  - Integration der aufgrund der Risikoanalyse identifizierten zusätzlichen Maßnahmen in das Sicherheitskonzept

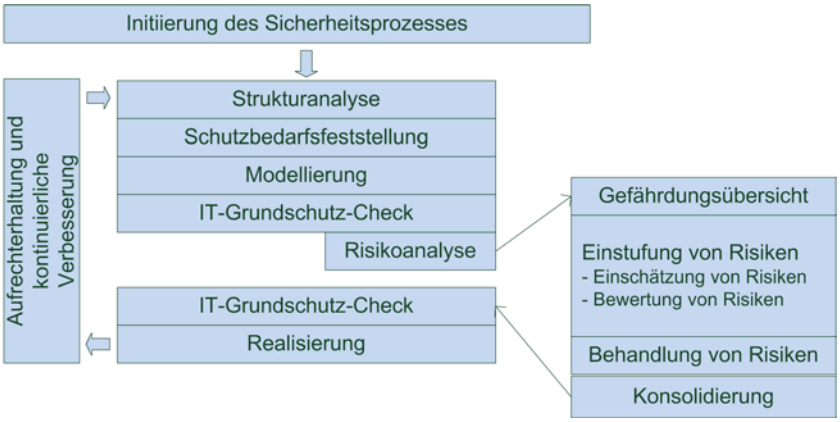


Abbildung 1: Integration der Risikoanalyse in den Sicherheitsprozess

In den internationalen Normen, insbesondere der ISO 31000, werden einige Begriffe anders belegt als es im deutschen Sprachraum üblich ist. Daher findet sich im Anhang eine Tabelle, in der die wesentlichen Begriffe aus ISO 31000 und dem 200-3 gegenübergestellt werden (siehe Tabelle 11).

1.4 Adressatenkreis

Dieses Dokument richtet sich an Sicherheitsverantwortliche, -beauftragte, -experten, -berater und alle Interessierte, die mit dem Management von oder der Durchführung von Risikoanalysen für die Informationssicherheit betraut sind.

Dieser Standard bietet sich an, wenn Unternehmen oder Behörden bereits erfolgreich mit der IT-Grundschutz-Methodik gemäß BSI-Standard 200-2 (siehe [BSI2]) arbeiten und möglichst direkt eine Risikoanalyse an die IT-Grundschutz-Analyse anschließen möchten. Abhängig von den Rahmenbedingungen einer Institution und der Art des Informationsverbunds kann es jedoch zweckmäßig sein, alternativ zum BSI-Standard 200-3 ein anderes etabliertes Verfahren oder eine angepasste Methodik für die Analyse von Informationsrisiken zu verwenden.

1.5 Anwendungsweise

Dieses Dokument beschreibt eine Methodik zur Analyse von Risiken. Diese kann benutzt werden, um ein IT-Grundschutz-Sicherheitskonzept zu ergänzen. Dabei wird die im IT-Grundschutz-Kompendium enthaltene Liste von elementaren Gefährdungen als Hilfsmittel verwendet. Es wird empfohlen, die in den Kapiteln 2 bis 8 dargestellte Methodik Schritt für Schritt durchzuarbeiten.

Im BSI-Standard 100-4 *Notfallmanagement* (siehe [BSI4]) ist für besonders kritische Ressourcen der Geschäftsprozesse der Institution ebenfalls eine Risikoanalyse vorgesehen, die sich von der hier beschriebenen nur in einigen Begriffen unterscheidet. Beide Risikoanalysen können effizient aufeinander abgestimmt werden. Es ist sinnvoll, dass sich alle Rollen in einer Institution, die sich mit Risikomanagement für einen spezifischen Bereich beschäftigen, miteinander abstimmen und vergleichbare Vorgehensweisen wählen.

2 Vorarbeiten zur Risikoanalyse

Bevor die eigentliche Risikoanalyse beginnt, sollten folgende Vorarbeiten abgeschlossen sein, die in der IT-Grundschutz-Methodik gemäß BSI-Standard 200-2 beschrieben sind:

- Es muss ein systematischer Informationssicherheitsprozess initiiert worden sein. Dieser dient dazu, die Aktivitäten im Bereich der Informationssicherheit strukturiert abzuarbeiten. Beispielsweise müssen geeignete Rollen und Aufgaben definiert werden.
- Gemäß Kapitel 3.3 der IT-Grundschutz-Methodik muss ein Geltungsbereich für die Sicherheitskonzeption definiert worden sein. Dieser Geltungsbereich wird im Folgenden als Informationsverbund bezeichnet.
- Für den Informationsverbund sollte eine Strukturanalyse gemäß Kapitel 8.1 der IT-Grundschutz-Methodik durchgeführt worden sein. Dadurch werden die wichtigsten Informationen über den Informationsverbund ermittelt, zum Beispiel Geschäftsprozesse, der Netzplan sowie eine Liste der wichtigsten Anwendungen mit Abhängigkeit von den IT-Systemen.
- Anschließend sollte eine Schutzbedarfsfeststellung gemäß Kapitel 8.2 der IT-Grundschutz-Methodik durchgeführt worden sein. Als Ergebnis liegen der Schutzbedarf der Geschäftsprozesse, Anwendungen, IT-Systeme, genutzten Räume sowie eine Liste der kritischen Kommunikationsverbindungen vor. Der Schutzbedarf bezieht sich jeweils auf die Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit und wird nach IT-Grundschutz normalerweise in den Stufen normal, hoch und sehr hoch festgelegt.
- Es sollte eine Modellierung gemäß Kapitel 8.3 der IT-Grundschutz-Methodik und Kapitel 2 des IT-Grundschutz-Kompendiums durchgeführt worden sein. Dabei wird für jedes Zielobjekt im Informationsverbund festgelegt, ob es passende IT-Grundschutz-Bausteine gibt und wie diese anzuwenden sind. Die in den einzelnen Bausteinen genannten Sicherheitsanforderungen und die daraus abgeleiteten Sicherheitsmaßnahmen bilden die Basis für das IT-Grundschutz-Sicherheitskonzept des betrachteten Informationsverbundes.
- Es sollte vor der Risikoanalyse ein IT-Grundschutz-Check gemäß Kapitel 7.7 oder 8.4 der IT-Grundschutz-Methodik durchgeführt werden. Dadurch wird festgestellt, welche Basis- und Standard-Sicherheitsanforderungen für den vorliegenden Informationsverbund bereits erfüllt sind und wo noch Defizite bestehen.

Als Ergebnis der Vorarbeiten liegt eine Liste der Zielobjekte vor, für die eine Risikoanalyse durchgeführt werden sollte ("betrachtete Zielobjekte"). Damit diese Aufgabe mit vertretbarem Aufwand geleistet werden kann, ist es wichtig, dass die Zielobjekte – gemäß IT-Grundschutz-Vorgehensweise – sinnvoll zu Gruppen zusammengefasst worden sind.

Falls trotz Gruppenbildung viele Zielobjekte einer Risikoanalyse unterzogen werden müssen, sollte eine geeignete Priorisierung vorgenommen werden:

- Falls für den IT-Grundschutz die Vorgehensweise "Standard-Absicherung" gewählt wurde, sollten vorrangig die übergeordneten Zielobjekte bearbeitet werden (insbesondere Geschäftsprozesse, Teilverbünde und gesamter Informationsverbund). Aus diesen Arbeiten ergeben sich oft wertvolle Anhaltspunkte für die Risikoanalysen der untergeordneten technischen Zielobjekte.

- Falls für den IT-Grundschutz die Vorgehensweise "Kern-Absicherung" gewählt wurde, sollten vorrangig die Zielobjekte mit dem höchsten Schutzbedarf bearbeitet werden.
- Falls für den IT-Grundschutz die Vorgehensweise "Basis-Absicherung" gewählt wurde, werden zunächst keine Risikoanalysen durchgeführt, sondern es werden als erstes nur die Basis-Anforderungen umgesetzt.

Von der hier beschriebenen Vorgehensweise kann abgewichen werden. Unter Umständen bietet es sich an, eine Risikoanalyse erst nach Erfüllung der IT-Grundschutz-Anforderungen durchzuführen. Dies kann beispielsweise bei Zielobjekten sinnvoll sein, die bereits im Einsatz sind und die hinreichend durch IT-Grundschutz-Bausteine dargestellt werden können. Als Entscheidungshilfe dazu, nach welchem Schritt eine Risikoanalyse sinnvoll ist, findet sich eine Zusammenstellung der Vor- und Nachteile der möglichen Zeitpunkte in Kapitel 8.5 der IT-Grundschutz-Methodik (siehe [BSI2]).

Hinweis: Bei den betrachteten Zielobjekten muss es sich nicht zwangsläufig um systemorientierte Zielobjekte (z. B. Anwendungen, IT-Systeme oder Räume) handeln. Vielmehr kann die Risikoanalyse auch auf Geschäftsprozessebene durchgeführt werden.

Zu den Vorarbeiten gehört auch, dass die Grundvoraussetzungen für die Risikoanalyse von der Institutionsleitung vorgegeben werden. Hierzu muss die Leitungsebene eine Richtlinie zum Umgang mit Risiken verabschieden. Diese sollte unter anderem folgende Aspekte umfassen:

- Unter welchen Voraussetzungen muss in jedem Fall eine Risikoanalyse durchgeführt werden?
- Welche Methodik, beziehungsweise welcher Standard, wird dazu eingesetzt, um die Risiken zu identifizieren, einzuschätzen, zu bewerten und zu behandeln?
- Wie wird die gewählte Methodik auf die speziellen Belange der Institution angepasst?
- Was sind die Risikoakzeptanzkriterien?
- Welche Organisationseinheiten sind für welche Teilaufgaben der Risikoanalyse verantwortlich? Sind Risiken den jeweiligen Risikoeigentümern zugeordnet?
- Auf welche Weise werden Risikoanalysen in den Sicherheitsprozess integriert, geschieht dies beispielsweise vor oder nach Umsetzung der IT-Grundschutz-Anforderungen?
- Welche Berichtspflichten bestehen im Rahmen von Risikoanalysen?
- In welchem Zeitrahmen muss die Risikoanalyse vollständig aktualisiert werden?

Da die Risikoakzeptanzkriterien einer Institution in entscheidendem Maße von deren Risikoneigung (Risikoappetit) abhängen, kann es sinnvoll sein, auch die Risikoneigung (siehe Kapitel 9) in der Richtlinie zu beschreiben. Möglicherweise ist sich eine Institution ihrer eigenen Risikoneigung nicht bewusst oder hat ungenaue Vorstellungen von diesem Begriff. In diesem Fall sollte die Leitungsebene eine Klärung und Entscheidung herbeiführen, gegebenenfalls sollte die Institution hierfür auf externe Experten zurückgreifen.

Die in der Richtlinie zur Risikoanalyse beschriebenen Vorgaben der Leitungsebene müssen konsequent umgesetzt werden, wenn Risiken bewertet und behandelt werden. Zweifelsfälle können auftreten, beispielsweise wenn es bei einem bestimmten Risiko nicht sinnvoll erscheint, die festgelegte Risikoneigung anzuwenden. Solche Ausnahmefälle sollten abgestimmt und dokumentiert werden.

Die Richtlinie zur Risikoanalyse sollte gemäß den Vorgaben des Informationssicherheitsmanagementsystems (siehe BSI-Standard 200-2 *IT-Grundschutz Methodik* [BSI2]) erstellt werden. Sie muss in regelmäßigen Abständen oder anlassbezogen auf ihre Aktualität hin überprüft und gegebenenfalls orientiert an den Zielen der Institution angepasst werden. Insbesondere sollte auch die eingesetzte Vorgehensweise zur Risikoanalyse regelmäßig überprüft werden. Die Richtlinie zur Risikoanalyse muss durch die Institutionsleitung freigegeben werden.

Beispiel 1:

Im Folgenden wird anhand einer fiktiven Institution, der RECPLAST GmbH, beispielhaft dargestellt, wie Risiken eingeschätzt, bewertet und behandelt werden können. Zu beachten ist, dass die Struktur der RECPLAST GmbH im Hinblick auf Informationssicherheit keineswegs optimal ist. Sie dient lediglich dazu, die Vorgehensweise bei der Durchführung von Risikoanalysen zu illustrieren.

Die RECPLAST GmbH ist eine fiktive Institution mit ca. 500 Mitarbeitern, von denen 130 an Bildschirmarbeitsplätzen arbeiten. Räumlich ist die RECPLAST GmbH aufgeteilt in zwei Standorte innerhalb von Bonn, wo unter anderem die administrativen und produzierenden Aufgaben wahrgenommen werden, und drei Vertriebsstandorte in Deutschland.

Das IT-Netz ist in mehrere Teilbereiche aufgeteilt. Für die Beispiele in dieser Risikoanalyse wird das Teilnetz A (vergleiche Abbildung 2 in Kapitel 4) näher betrachtet. Der Zugang zum Teilnetz A ist durch die Firewall N1 abgesichert. Die Server S1 (Virtualisierungsserver) und S5 werden durch einzelne Switches angebunden.

Der Virtualisierungsserver S1 stellt verschiedene Dienste zur Verfügung, z. B. werden dort in virtuellen Maschinen File- und E-Mail-Server betrieben. Diese Anwendungen haben teilweise einen hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit. Durch das Maximumprinzip gilt für den Virtualisierungsserver S1 der höchste Schutzbedarf der zur Verfügung gestellten virtuellen Maschinen bzw. IT-Anwendungen. Um die Stunden der Mitarbeiter zu erfassen, verwendet die RECPLAST GmbH eine Softwarelösung, die als Webanwendung implementiert ist. Für die Datenhaltung nutzt diese eine Datenbank, die im Datenbankmanagementsystem (A1) auf dem Server S5 betrieben wird.

Darüber hinaus betreibt die RECPLAST GmbH eine Reihe von Servern, die dazu eingesetzt werden, alle IT-Systeme und darauf betriebenen Anwendungen kontinuierlich zu überwachen.

Beispiel 2:

Das fiktive Unternehmen MUSTERENERGIE GmbH betreibt eine Smart Meter Gateway Infrastruktur (intelligentes Netz). Kernbausteine einer solchen Infrastruktur sind intelligente Messsysteme, auch "Smart Metering Systems" genannt. Das Smart Meter Gateway (SMGW) stellt dabei die zentrale Kommunikationseinheit dar. Es kommuniziert im lokalen Bereich beim Endkunden mit den elektronischen Zählern (Local Metrological Network, LMN-Bereich), mit Geräten aus dem Home Area Network (HAN-Bereich) und im Wide Area Network (WAN-Bereich) mit autorisierten Marktteilnehmern. Außerdem ermöglicht das SMGW die Verbindungsaufnahme von lokalen Geräten des HAN über das WAN mit autorisierten Marktteilnehmern.

Für die Installation, Inbetriebnahme, den Betrieb, die Wartung und Konfiguration des SMGW ist der Smart Meter Gateway Administrator (SMGW Admin) verantwortlich. Da es sich hierbei teilweise um sensible Informationen handelt, ist der Schutz dieser Informationen wichtig. Daher muss sichergestellt sein, dass der IT-Betrieb beim SMGW Admin sicher erfolgt.

Für die Beispiele in dieser Risikoanalyse wird neben Teilnetz A der RECPLAST GmbH auch die Smart Meter Gateway Administration der MUSTERENERGIE GmbH näher betrachtet.

3 Übersicht über die elementaren Gefährdungen

Das BSI hat aus den vielen spezifischen Einzelgefährdungen der IT-Grundschutz-Bausteine die generellen Aspekte herausgearbeitet und in 47 elementare Gefährdungen überführt, die im IT-Grundschutz-Kompendium aufgeführt sind. Bei der Erstellung der Übersicht der elementaren Gefährdungen wurden die im Folgenden beschriebenen Ziele verfolgt. Elementare Gefährdungen sind

- für die Verwendung bei der Risikoanalyse optimiert,
- produktneutral (immer), technikneutral (möglichst, bestimmte Techniken prägen so stark den Markt, dass sie auch die abstrahierten Gefährdungen beeinflussen),
- kompatibel mit vergleichbaren internationalen Katalogen und Standards und
- nahtlos in den IT-Grundschutz integriert.

Da die elementaren Gefährdungen hauptsächlich die effiziente Durchführung von Risikoanalysen ermöglichen sollen, wurde der Fokus darauf gelegt, tatsächliche Gefahren zu benennen. Gefährdungen, die überwiegend die fehlende oder unzureichende Umsetzung von Sicherheitsmaßnahmen thematisieren und somit auf indirekte Gefahren verweisen, wurden bewusst nicht benannt. Bei der Erarbeitung der Übersicht der elementaren Gefährdungen wurde mitbetrachtet, welcher Grundwert der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) durch die jeweilige Gefährdung beschädigt würde. Da diese Information bei verschiedenen Schritten der Sicherheitskonzeption von Interesse ist, wird sie in der folgenden Tabelle mit aufgeführt. Nicht alle elementaren Gefährdungen lassen sich auf genau einen Grundwert abbilden, gleichwohl betreffen verschiedene Gefährdungen mehrere Grundwerte. Dabei ist dies so zu interpretieren, dass durch die jeweilige Gefährdung die dazu aufgeführten Grundwerte direkt beeinträchtigt werden. Bei vielen Gefährdungen lässt sich diskutieren, inwieweit alle drei Grundwerte betroffen sein könnten, weil sich auch indirekte Auswirkungen ableiten lassen. So wird z. B. zu G 0.1 *Feuer* als einziger betroffener Grundwert "Verfügbarkeit" genannt. Natürlich könnte ein Feuer einen Datenträger auch so beschädigen, dass die abgespeicherten Informationen zwar noch vorhanden sind, aber deren Integrität verletzt ist. Ein anderes Szenario könnte sein, dass bei einem Brand vertrauliche Unterlagen durch Rettungsmaßnahmen für Unbefugte zugänglich wären. Dies wären zwar indirekte Auswirkungen auf die Grundwerte Vertraulichkeit und Integrität, aber nur die Verfügbarkeit ist unmittelbar beeinträchtigt.

In der folgenden Tabelle findet sich die Übersicht über die elementaren Gefährdungen sowie die Nennung der hauptsächlich betroffenen Grundwerte. Dabei steht C für Confidentiality (Vertraulichkeit), I für Integrity (Integrität) und A für Availability (Verfügbarkeit).

	Gefährdung	Grundwert
G 0.1	Feuer	A
G 0.2	Ungünstige klimatische Bedingungen	I,A
G 0.3	Wasser	I,A
G 0.4	Verschmutzung, Staub, Korrosion	I,A
G 0.5	Naturkatastrophen	A
G 0.6	Katastrophen im Umfeld	A
G 0.7	Großereignisse im Umfeld	C,I,A
G 0.8	Ausfall oder Störung der Stromversorgung	I,A
G 0.9	Ausfall oder Störung von Kommunikationsnetzen	I,A
G 0.10	Ausfall oder Störung von Versorgungsnetzen	A
G 0.11	Ausfall oder Störung von Dienstleistern	C,I,A
G 0.12	Elektromagnetische Störstrahlung	I,A
G 0.13	Abfangen kompromittierender Strahlung	C
G 0.14	Ausspähen von Informationen / Spionage	C
G 0.15	Abhören	C
G 0.16	Diebstahl von Geräten, Datenträgern und Dokumenten	C,A
G 0.17	Verlust von Geräten, Datenträgern und Dokumenten	C,A
G 0.18	Fehlplanung oder fehlende Anpassung	C,I,A
G 0.19	Offenlegung schützenswerter Informationen	C
G 0.20	Informationen aus unzuverlässiger Quelle	C,I,A
G 0.21	Manipulation von Hard- und Software	C,I,A
G 0.22	Manipulation von Informationen	I
G 0.23	Unbefugtes Eindringen in IT-Systeme	C,I
G 0.24	Zerstörung von Geräten oder Datenträgern	A
G 0.25	Ausfall von Geräten oder Systemen	A
G 0.26	Fehlfunktion von Geräten oder Systemen	C,I,A
G 0.27	Ressourcenmangel	A
G 0.28	Software-Schwachstellen oder –Fehler	C,I,A
G 0.29	Verstoß gegen Gesetze oder Regelungen	C,I,A
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	C,I,A
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	C,I,A
G 0.32	Missbrauch von Berechtigungen	C,I,A
G 0.33	Personalausfall	A
G 0.34	Anschlag	C,I,A
G 0.35	Nötigung, Erpressung oder Korruption	C,I,A
G 0.36	Identitätsdiebstahl	C,I,A
G 0.37	Abstreiten von Handlungen	C,I
G 0.38	Missbrauch personenbezogener Daten	C
G 0.39	Schadprogramme	C,I,A
G 0.40	Verhinderung von Diensten (Denial of Service)	A
G 0.41	Sabotage	A
G 0.42	Social Engineering	C,I
G 0.43	Einspielen von Nachrichten	C,I
G 0.44	Unbefugtes Eindringen in Räumlichkeiten	C,I,A
G 0.45	Datenverlust	A
G 0.46	Integritätsverlust schützenswerter Informationen	I
G 0.47	Schädliche Seiteneffekte IT-gestützter Angriffe	C, I, A

Tabelle 1: Übersicht über die elementaren Gefährdungen mit den jeweils betroffenen Grundwerten

4 Erstellung einer Gefährdungsübersicht

Ziel der folgenden Arbeitsschritte ist es, als Ausgangspunkt für die Risikoanalyse eine Übersicht über die Gefährdungen zu erstellen, die auf die betrachteten Zielobjekte des Informationsverbunds einwirken. Als Ergebnis der Vorarbeiten (siehe Kapitel 2) liegt eine Liste von (priorisierten) Zielobjekten vor, für die eine Risikoanalyse durchgeführt werden sollte. Diese dient als Grundlage für die Erstellung der Gefährdungsübersicht. Ergänzt wird diese Liste um das übergeordnete Zielobjekt "Informationsverbund", sofern dieses Zielobjekt nicht ohnehin bereits in der Liste enthalten ist. Bei der Ermittlung von Gefährdungen geht das BSI zweistufig vor. Zunächst werden die relevanten elementaren Gefährdungen identifiziert und darauf aufbauend werden weitere mögliche Gefährdungen (zusätzliche Gefährdungen) ermittelt, die über die elementaren Gefährdungen hinausgehen.

4.1 Ermittlung von elementaren Gefährdungen

Wie bei der Ermittlung von elementaren Gefährdungen vorgegangen wird, ist davon abhängig, ob das betrachtete Zielobjekt hinreichend mit bestehenden Bausteinen des IT-Grundschutz-Kompendiums abgebildet werden kann oder nicht. Für bestehende Bausteine wurde bereits vorab eine Risikoanalyse durchgeführt und damit wurden für diese Bausteine bereits die relevanten elementaren Gefährdungen ermittelt, die als Ausgangspunkt der Gefährdungsanalyse verwendet werden können. Für jedes Zielobjekt werden Nummer und Titel dieser Gefährdungen zusammengetragen und dem jeweiligen Zielobjekt zugeordnet. Darüber hinaus wird die Liste der elementaren Gefährdungen herangezogen und es wird geprüft, ob weitere elementare Gefährdungen für das Zielobjekt relevant sind, also *prinzipiell* zu einem *nennenswerten Schaden* führen können. Dafür ist jede weitere elementare Gefährdung daraufhin zu bewerten, ob diese direkt, indirekt oder gar nicht auf das Zielobjekt einwirken kann:

- "Direkt relevant" bedeutet hier, dass die jeweilige Gefährdung auf das betrachtete Zielobjekt einwirken kann und deshalb im Rahmen der Risikoanalyse behandelt werden muss.
- "Indirekt relevant" bedeutet hier, dass die jeweilige Gefährdung zwar auf das betrachtete Zielobjekt einwirken kann, in ihrer potenziellen Wirkung aber nicht über andere (allgemeinere) Gefährdungen hinausgeht. In diesem Fall muss die jeweilige Gefährdung für dieses Zielobjekt nicht gesondert im Rahmen der Risikoanalyse behandelt werden.
- "Nicht relevant" bedeutet hier, dass die jeweilige Gefährdung nicht auf das betrachtete Zielobjekt einwirken kann und deshalb für dieses Zielobjekt im Rahmen der Risikoanalyse nicht behandelt werden muss.

Gefährdungen, die für ein bestimmtes Zielobjekt nur "indirekt relevant" oder "nicht relevant" sind, können aber natürlich für andere Zielobjekte im selben Informationsverbund durchaus "direkt relevant" sein.

In der Praxis hat der Typ des jeweiligen Zielobjekts einen wesentlichen Einfluss darauf, welche elementaren Gefährdungen überhaupt darauf anwendbar sind. So wird die Gefährdung G 0.28 *Software-Schwachstellen oder -Fehler* nur selten für einen Büroraum relevant sein, sondern eher für die darin betriebenen Clients. Gefährdungen, die sich nicht auf konkrete technische Komponenten beziehen, beispielsweise G 0.29 *Verstoß gegen Gesetze oder Regelungen*, eignen sich meist für Zielobjekte vom Typ Anwendung, Geschäftsprozess oder Informationsverbund.

Beispiel:

Wird ein spezifisches Server-Betriebssystem betrachtet, ist beispielsweise die elementare Gefährdung G 0.25 *Ausfall von Geräten oder Systemen* eine relevante Gefährdung, gegen die unter Umständen spezifische Sicherheitsmaßnahmen zu ergreifen sind. Dagegen ist die elementare Gefährdung G 0.1 *Feuer* für ein spezifisches Server-Betriebssystem irrelevant. Ein Betriebssystem bietet keine

spezifischen Schutzmaßnahmen gegen Feuer, es würden durch die Betrachtung von G 0.1 *Feuer* keine neuen Aspekte gegenüber G 0.25 *Ausfall von Geräten oder Systemen* entstehen.

Gefährdung	Grundwerte	Wirkung und Relevanz	Kommentar
G 0.1 Feuer	Verfügbarkeit	Indirekte Wirkung / nicht relevant	Die Gefährdung für ein Betriebssystem durch Feuer ist irrelevant, es würden durch die Betrachtung von G 0.1 *Feuer* keine neuen Aspekte gegenüber G 0.25 *Ausfall von Geräten oder Systemen* abgedeckt.
G 0.9 Ausfall oder Störung von Kommuni-kations-netzen	Verfügbarkeit, Integrität	Indirekte Wirkung / nicht relevant	Die Gefährdung für ein Betriebssystem durch *Ausfall oder Störung von Kommunikationsnetzen* ist indirekt, es würden durch die Betrachtung von G 0.9 keine neuen Aspekte gegenüber G 0.26 *Fehlfunktionen von Geräten oder Systemen* entstehen. Ein Betriebssystem bietet keine spezifischen Schutzmaßnahmen gegen G 0.9, die Gefährdung ist somit hier nicht relevant. Es sind keine spezifischen Maßnahmen erforderlich.
G 0.25 Ausfall von Geräten oder Systemen	Verfügbarkeit	Direkte Wirkung / relevant	Die Gefährdung durch G 0.25 *Ausfall von Geräten oder Systemen* wirkt direkt auf ein Betriebssystem ein. Daher sind Maßnahmen gegen G 0.25 *Ausfall von Geräten und Systemen* zu prüfen.
G 0.26 Fehlfunktion von Geräten oder Systemen	Vertraulichkeit, Verfügbarkeit, Integrität	Direkte Wirkung / relevant	Die Gefährdung durch G 0.26 *Fehlfunktionen von Geräten oder Systemen* wirkt direkt auf ein Betriebssystem ein. Daher sind Maßnahmen gegen G 0.26 Fehlfunktionen von Geräten und Systemen zu prüfen.

Tabelle 2: Beispiel zur Ermittlung elementarer Gefährdungen für ein Server-Betriebssystem

Kann das betrachtete Zielobjekt nicht hinreichend mit bestehenden Bausteinen des IT-Grundschutz-Kompendiums abgebildet werden, da es sich um Themenbereiche handelt, die bisher im IT-Grundschutz-Kompendium noch nicht oder nicht ausreichend abgedeckt sind, um den betrachteten Informationsverbund modellieren zu können, dann wird die Liste der 47 elementaren Gefährdungen herangezogen und für jedes Zielobjekt jeweils geprüft, welche Gefährdungen relevant sind. Hierbei kann dieselbe Vorgehensweise wie weiter vorhin beschrieben angewendet werden.

Als Ergebnis der vorangegangenen Schritte liegt eine Tabelle vor, in der jedem Zielobjekt eine Liste mit relevanten elementaren Gefährdungen zugeordnet ist. Um die nachfolgende Analyse zu erleichtern, sollte in der Tabelle für jedes Zielobjekt der Schutzbedarf vermerkt werden, der im Rahmen der Schutzbedarfsfeststellung in den drei Grundwerten Vertraulichkeit, Integrität und Verfügbarkeit ermittelt wurde. Für das übergeordnete Zielobjekt *Informationsverbund* kann diese Zuordnung entfallen.

Im Folgenden wird anhand der zwei Beispiele dargestellt, wie die Gefährdungsübersicht anhand von elementaren Gefährdungen erstellt werden kann.

Beispiel 1:

Die RECPLAST GmbH betreibt an ihrem Standort in Bad Godesberg ein zentral administriertes Netz mit 130 angeschlossenen Arbeitsplätzen. Die Arbeitsplatzrechner sind mit den üblichen Büro-Anwendungen (Standardsoftware für Textverarbeitung, Tabellenkalkulation und Präsentation) und Client-Software für E-Mail und Internet-Nutzung ausgestattet. Zusätzlich gibt es je nach Aufgabengebiet auf verschiedenen Arbeitsplatzrechnern Spezialsoftware.

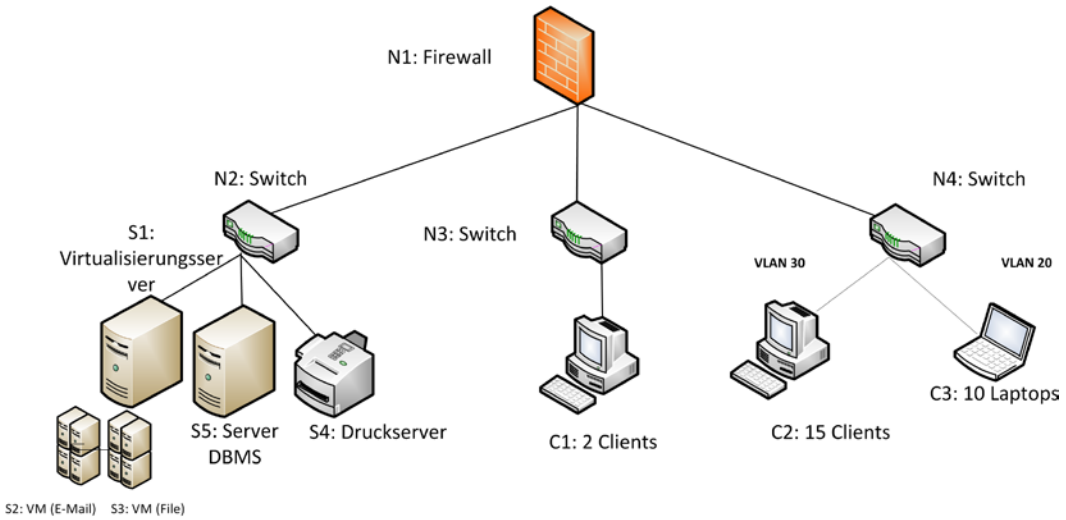


Abbildung 2: Ausschnitt aus einem Netzplan (RECPLAST Teilnetz A)

Im Rahmen der Schutzbedarfsfeststellung ist für folgende Zielobjekte (siehe Tabelle 3) hoher bzw. sehr hoher Schutzbedarf in mindestens einem der drei Grundwerte (Vertraulichkeit, Integrität oder Verfügbarkeit) festgestellt worden. Somit müssen diese einer Risikoanalyse unterzogen werden.

- Firewall N1
- Switches N2, N3 und N4,
- Virtualisierungsserver S1, virtuelle Maschinen S2 und S3, DBMS-Server (S5) und Datenbankmanagementsystem A1 (kurz Datenbank A1),
- Laptops C3 und Clients C1

Im Folgenden findet sich ein Auszug aus RECPLAST GmbH Teilnetz A**:**

Nummer	Titel des Bausteins	Zielobjekt
ISMS.1, ORP.1 etc.	*Sicherheitsmanagement, Organisation etc.*	IV
INF.2	*Rechenzentrum*	M.1, M.2
INF.7	*Büroraum*	M.3
NET.3.2	*Firewall*	N1
NET.3.1	*Router und Switches*	N2, N4
NET.3.1	*Router und Switches*	N3
SYS.1.5	*Virtualisierung*	S1
APP.5.1	*Groupware*	S2 (VM1)
APP.3.3	*Fileserver*	S3 (VM2)
SYS.1.2.2	*Windows Server 2012*	S5
APP.4.3	*Relationale Datenbanksysteme*	A1
SYS.2.2	*Windows-Clients*	C1
SYS.2.3	*Clients unter Unix (Laptops)*	C3

Tabelle 3: Liste der betrachteten Zielobjekte (Auszug)

Beispiel 2:

Bei der Modellierung des Informationsverbundes, der der Smart Meter Gateway Administration zugrunde liegt, ist festgestellt worden, dass dem Zielobjekt "Smart Meter Gateway Administration Zx" kein IT-Grundschutz-Baustein zugeordnet werden kann. Dieses muss daher ebenfalls einer Risikoanalyse unterzogen werden.

(Auszug Smart Meter Gateway Administration)

Nummer	Titel des Bausteins	Zielobjekt
-	-	Smart Meter Gateway Administration Zx

Tabelle 4: Liste der betrachteten Zielobjekte (Auszug)

Die nachfolgenden Tabellen stellen eine Übersicht von relevanten elementaren Gefährdungen für die betrachteten Zielobjekte (Virtualisierungsserver S1, Datenbank A1) und Smart Meter Gateway Administration Zx dar. Sie dienen als Ausgangspunkt für die nachfolgende *Ermittlung zusätzlicher Gefährdungen*.

Virtualisierungsserver S1
Vertraulichkeit: hoch Integrität: hoch Verfügbarkeit: hoch
G 0.14 *Ausspähen von Informationen / Spionage*
G 0.15 *Abhören*
G 0.18 *Fehlplanung oder fehlende Anpassung*
G 0.19 *Offenlegung schützenswerter Informationen*
G 0.21 *Manipulation von Hard- oder Software*
G 0.22 *Manipulation von Informationen*
G 0.23 *Unbefugtes Eindringen in IT-Systeme*
G 0.25 *Ausfall von Geräten oder Systemen*
G 0.26 *Fehlfunktion von Geräten oder Systemen*
G 0.28 *Software-Schwachstellen oder -Fehler*
G 0.30 *Unberechtigte Nutzung oder Administration von Geräten und Systemen*
G 0.31 *Fehlerhafte Nutzung oder Administration von Geräten und Systemen*
G 0.32 *Missbrauch von Berechtigungen*
G 0.40 *Verhinderung von Diensten (Denial of Service)*
G 0.43 *Einspielen von Nachrichten*
G 0.45 *Datenverlust*
G 0.46 *Integritätsverlust schützenswerter Informationen*

Tabelle 5: Gefährdungsübersicht für das Zielobjekt S1 (Auszug)

Datenbank A1
Vertraulichkeit: hoch Integrität: hoch Verfügbarkeit: hoch
G 0.14 *Ausspähen von Informationen / Spionage* G 0.15 *Abhören* G 0.18 *Fehlplanung oder fehlende Anpassung* G 0.19 *Offenlegung schützenswerter Informationen* G 0.20 *Informationen aus unzuverlässiger Quelle* G 0.21 *Manipulation von Hard- und Software* G 0.22 *Manipulation von Informationen* G 0.23 *Unbefugtes Eindringen in IT-Systeme* G 0.25 *Ausfall von Geräten oder Systemen* G 0.26 *Fehlfunktion von Geräten oder Systemen* G 0.27 *Ressourcenmangel* G 0.28 *Software-Schwachstellen oder –Fehler* G 0.30 *Unberechtigte Nutzung oder Administration von Geräten und Systemen* G 0.31 *Fehlerhafte Nutzung oder Administration von Geräten und Systemen* G 0.32 *Missbrauch von Berechtigungen* G 0.37 *Abstreiten von Handlungen* G 0.39 *Schadprogramme* G 0.40 *Verhinderung von Diensten (Denial of Service)* G 0.43 *Einspielen von Nachrichten* G 0.45 *Datenverlust* G 0.46 *Integritätsverlust schützenswerter Informationen*

Tabelle 6: Gefährdungsübersicht für das Zielobjekt A1 (Auszug)

Smart Meter Gateway Administration Zx
Vertraulichkeit: hoch Integrität: hoch Verfügbarkeit: hoch
G 0.18 Fehlplanung oder fehlende Anpassungen *G 0.21 Manipulation von Hard- oder Software* *G 0.22 Manipulation von Informationen* *G 0.23 Unbefugtes Eindringen in IT-Systeme* *G 0.25 Ausfall von Geräten oder Systemen* *G 0.26 Fehlfunktion von Geräten oder Systemen* *G 0.28 Software-Schwachstellen oder -Fehler* *G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen* *G 0.43 Einspielen von Nachrichten* *usw.*

Tabelle 7: Gefährdungsübersicht für das Zielobjekt Zx (Auszug)

4.2 Ermittlung zusätzlicher Gefährdungen

Für die betrachteten Zielobjekte gibt es unter Umständen einzelne zusätzliche Gefährdungen, die über die elementaren Gefährdungen hinausgehen und sich aus dem spezifischen Einsatzszenario oder Anwendungsfall ergeben. Diese müssen ebenfalls berücksichtigt werden.

Für die Informationssicherheit *relevante Gefährdungen* sind solche,

- die zu einem nennenswerten Schaden führen können und
- die im vorliegenden Anwendungsfall und Einsatzumfeld realistisch sind.

Die elementaren Gefährdungen wurden so ausgewählt, dass sie eine kompakte, gleichzeitig angemessene und in typischen Szenarien vollständige Grundlage für Risikoanalysen bieten. Daher sollte der Fokus bei der Ermittlung zusätzlicher Gefährdungen nicht darauf liegen, weitere elementare Gefährdungen zu identifizieren. Es kann aber sinnvoll sein, spezifische Aspekte einer elementaren Gefährdung zu betrachten, da dies es erleichtern kann, spezifische Maßnahmen zu identifizieren.

Hinweis: Falls eine Institution im Rahmen dieses Schrittes eine weitere *generische* Gefährdung identifiziert, die bisher nicht im IT-Grundschutz-Kompendium enthalten ist, sollte sie dies dem BSI mitteilen, damit der Katalog der elementaren Gefährdungen entsprechend erweitert werden kann.

Bei der Ermittlung zusätzlicher relevanter Gefährdungen sollte der Schutzbedarf des jeweiligen Zielobjekts in Bezug auf die drei *Grundwerte* der Informationssicherheit *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* berücksichtigt werden:

- Hat das Zielobjekt in einem bestimmten Grundwert den Schutzbedarf *sehr hoch*, sollten vorrangig solche Gefährdungen gesucht werden, die diesen Grundwert beeinträchtigen.
- Auch wenn das Zielobjekt in einem bestimmten Grundwert den Schutzbedarf *hoch* hat, sollten solche Gefährdungen gesucht werden, die diesen Grundwert beeinträchtigen.
- Hat das Zielobjekt in einem bestimmten Grundwert den Schutzbedarf *normal*, sind die empfohlenen Sicherheitsanforderungen für diesen Grundwert in der Regel ausreichend, sofern das Zielobjekt mit den existierenden Bausteinen des IT-Grundschutzes modelliert werden kann.

Unabhängig vom Schutzbedarf des betrachteten Zielobjekts ist die Identifikation zusätzlicher relevanter Gefährdungen besonders wichtig, wenn es im IT-Grundschutz-Kompendium keinen geeigneten Baustein für das Zielobjekt gibt oder wenn das Zielobjekt in einem Einsatzszenario (Umgebung, Anwendung) betrieben wird, das im IT-Grundschutz-Kompendium nicht vorgesehen ist.

Hinweise, welche Fragestellungen bei der Identifikation zusätzlicher Gefährdungen betrachtet werden sollen, finden sich im Anhang (siehe Kapitel 9).

In der Praxis ist es oft so, dass zusätzliche Gefährdungen gleich mehrere Zielobjekte betreffen. Die identifizierten zusätzlichen Gefährdungen werden in der Gefährdungsübersicht ergänzt.

Wichtig: Wenn relevante Gefährdungen nicht berücksichtigt werden, kann dies zu Lücken im resultierenden Sicherheitskonzept führen. Im Zweifelsfall sollte daher sorgfältig analysiert werden, ob und (wenn ja) welche Gefährdungen noch fehlen. Hierbei ist es oft ratsam, auf externe Beratungsdienstleistungen zurückzugreifen.

In der Praxis hat es sich bewährt, zur Identifikation zusätzlicher Gefährdungen ein gemeinsames Brainstorming mit allen beteiligten Mitarbeitern durchzuführen. Es sollten Informationssicherheitsbeauftragte, Fachverantwortliche, Administratoren und Benutzer des jeweils betrachteten Zielobjekts und gegebenenfalls auch externe Sachverständige beteiligt werden. Der Arbeitsauftrag an die Teilnehmer sollte klar formuliert sein und die Zeit für das Brainstorming begrenzt werden. Ein Experte für Informationssicherheit sollte das Brainstorming moderieren.

Beispiel (Auszug RECPLAST)

Im Rahmen eines Brainstormings identifiziert das Unternehmen RECPLAST unter anderem folgende zusätzliche Gefährdungen:

Gesamter Informationsverbund
G z.1 *Manipulation durch Familienangehörige und Besucher*
Familienangehörige und Besucher haben zeitweise Zutritt zu bestimmten Räumlichkeiten des Unternehmens. Es besteht die Gefahr, dass diese Personen dies als Gelegenheit nutzen, unerlaubte Veränderungen an Hardware, Software oder Informationen vorzunehmen. Diese zusätzliche Gefährdung konkretisiert die elementaren Gefährdungen G 0.21 *Manipulation von Hard- oder Software* und G 0.22 *Manipulation von Informationen.*
usw.

Switch N3
Vertraulichkeit: Normal Integrität: Normal Verfügbarkeit: hoch
G z.2 *Beschädigung von Informationstechnik im Fertigungsbereich*
Der Client C1 und der Switch N3 werden im Fertigungsbereich des Unternehmens betrieben und sind deshalb besonderen physischen Gefahren ausgesetzt. Die Geräte können beschädigt, zerstört oder deren Lebensdauer reduziert werden. (Konkretisierung von G 0.24 *Zerstörung von Geräten oder Datenträgern*)
usw.

Datenbank A1
Vertraulichkeit: hoch Integrität: hoch Verfügbarkeit: hoch
Im Rahmen des Brainstormings wurden keine zusätzlichen Gefährdungen identifiziert, allerdings wurde festgestellt, dass zusätzliche Sicherheitsanforderungen erforderlich sind, um die Gefährdungen G 0.28 *Software-Schwachstellen oder -Fehler* und G 0.32 *Missbrauch von Berechtigungen* bei erhöhtem Schutzbedarf zu reduzieren. Dieses Ergebnis wird für den Arbeitsschritt *Behandlung von Risiken* vorgemerkt.

5 Risikoeinstufung

5.1 Risikoeinschätzung

Nachdem alle relevanten Gefährdungen identifiziert worden sind (siehe Kapitel 4), wird im nächsten Schritt das Risiko ermittelt, das von einer Gefährdung ausgeht. Wie hoch dieses Risiko ist, hängt sowohl von der Eintrittshäufigkeit (Eintrittseinschätzung) der Gefährdung als auch von der Höhe des Schadens ab, der dabei droht. Bei der Risikoeinschätzung müssen daher beide Einflussgrößen berücksichtigt werden.

Um Risiken mit angemessenem Aufwand einzuschätzen, gibt es kein einfaches allgemeingültiges Konzept. Der Risikoanteil *Schadenshöhe* kann nur von der Institution selbst eingeschätzt werden. Hierbei geht es darum, wie sich der Eintritt einer Gefährdung auswirken kann, d. h. welche Schäden finanzieller und anderer Art, welche direkten Schäden und welche Folgeschäden entstehen können. Darin geht auch ein, ob, mit welchem Aufwand und in welcher Zeit der Schaden zu beheben ist.

Die *Eintrittshäufigkeit* muss durch geeignetes Fachpersonal eingeschätzt werden und kann durch Statistiken und eigene Erfahrungen unterstützt werden. Bei Statistiken muss allerdings beachtet werden, unter welchen Randbedingungen sie entstanden sind, da auch Statistiken für einen speziellen Anwendungszweck erstellt worden sind und daher nicht ohne Weiteres auf die speziellen Belange der Institution übertragen werden können. Außerdem ist die Interpretation von statistischen Ergebnissen prinzipiell mit Unsicherheiten behaftet.

Grundsätzlich können Risiken entweder qualitativ oder quantitativ betrachtet werden. Die quantitative Risikobetrachtung ist sehr aufwändig und setzt umfangreiches statistisches Datenmaterial voraus. Solche umfangreichen Erfahrungswerte fehlen in den meisten Fällen im sehr dynamischen Umfeld der Informationssicherheit. Daher ist es in den meisten Fällen praktikabler, sowohl für die Eintrittshäufigkeit als auch für die potentielle Schadenshöhe mit qualitativen Kategorien zu arbeiten. Pro Dimension sollten dabei nicht mehr als fünf Kategorien gewählt werden.

Um Risiken einzuschätzen, nutzt der IT-Grundschutz die im Folgenden beschriebenen Kategorien. Jede Institution kann sowohl die Anzahl der Stufen als auch die Kriterien individuell festlegen. Sie sollte die Einteilungen nutzen, die zu ihrem Managementsystem am Besten passt.

- Eintrittshäufigkeit: selten, mittel, häufig, sehr häufig
- Potentielle Schadenshöhe: vernachlässigbar, begrenzt, beträchtlich, existenzbedrohend

Hinweis: Jede Institution sollte insbesondere die Beschreibungen der Kategorien mit den Fachabteilungen abstimmen, damit deren Bedeutung für alle Mitarbeiter einfach nachvollziehbar ist. Wenn ein konkretes Risiko von zwei unterschiedlichen Mitarbeitern einer Institution eingeschätzt wird, sollte dasselbe Ergebnis dabei herauskommen.

Eintrittshäufigkeit / Beschreibung	
selten	Ereignis könnte nach heutigem Kenntnisstand höchstens alle 5 Jahre eintreten.
mittel	Ereignis tritt einmal alle 5 Jahre bis einmal im Jahr ein.
häufig	Ereignis tritt einmal im Jahr bis einmal pro Monat ein.
sehr häufig	Ereignis tritt mehrmals im Monat ein.

Tabelle 8: Kategorisierung von Eintrittshäufigkeiten

Schadenshöhe / Schadensauswirkungen	
vernachlässigbar	Die Schadensauswirkungen sind gering und können vernachlässigt werden.
begrenzt	Die Schadensauswirkungen sind begrenzt und überschaubar.
beträchtlich	Die Schadensauswirkungen können beträchtlich sein.
existenzbedrohend	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Tabelle 9: Kategorisierung von Schadensauswirkungen

Es gibt Institutionen, die mit stärker differenzierten Kategorien arbeiten, um damit dem Bedarf in verschiedenen Abteilungen oder Geschäftsprozessen gerecht zu werten. In der Praxis werden aber häufig nur wenige Kategorien pro Dimension verwendet. Die Mehrheit der Anwender neigt sogar dazu, de-facto mit nur zwei Kategorien pro Dimension zu arbeiten, beispielsweise "begrenzt" und "beträchtlich".

5.2 Risikobewertung

Anhand der zuvor definierten Kategorien für die potentielle Schadenshöhe sowie der Klassifikation für Eintrittshäufigkeiten von Gefährdungen legt das BSI folgende Risikomatrix (siehe Abbildung 3) fest. Sie dient lediglich dazu, die nachfolgenden Beispiele zu veranschaulichen und sollte auf die eigenen Bedürfnisse angepasst werden

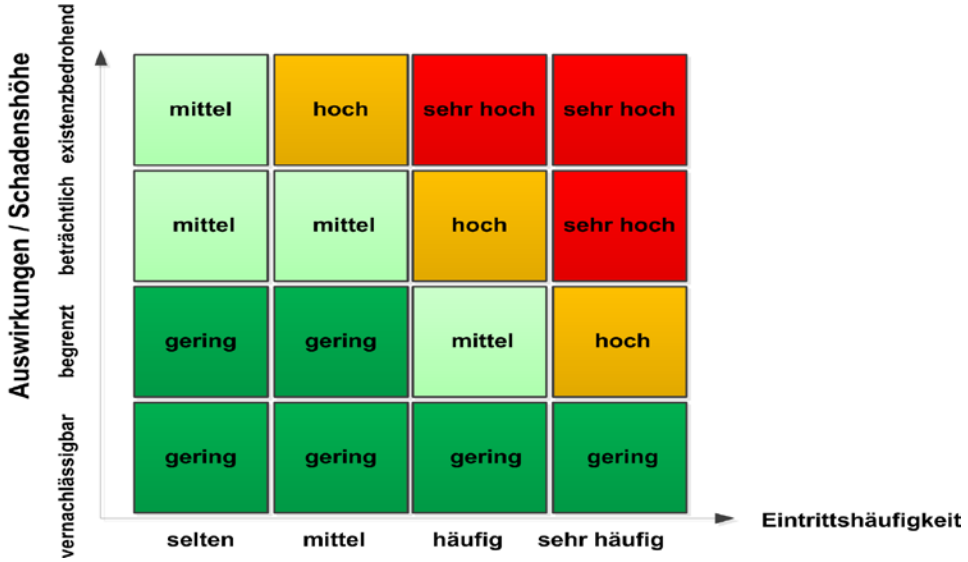


Abbildung 3: Matrix zur Einstufung von Risiken

Risikokategorien	
gering	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten einen ausreichenden Schutz. In der Praxis ist es üblich, geringe Risiken zu akzeptieren und die Gefährdung dennoch zu beobachten.
mittel	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen reichen möglicherweise nicht aus.
hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen

	Gefährdung.
sehr hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung. In der Praxis werden sehr hohe Risiken selten akzeptiert.

Tabelle 10: Definition von Risikokategorien

Nachdem Risiken identifiziert, eingeschätzt und bewertet worden sind, ist das weitere Vorgehen (Risikobehandlungsstrategie) von Institution zu Institution sehr unterschiedlich. Eine generelle Empfehlung zur Auswahl einer bestimmten Behandlungsstrategie, kann das BSI nicht geben, da viele individuelle Aspekte betrachtet werden müssen. Insbesondere hängt die Risikobehandlungsstrategie sehr stark vom Risikoappetit der jeweiligen Institution ab (siehe Kapitel 9).

Hinweis: Im Rahmen der Risikoeinstufung kommen oftmals erste Ideen zur Sprache, mit welchen Sicherheitsmaßnahmen den Gefährdungen begegnet werden kann. Diese Vorschläge sind für die nachfolgenden Arbeitsschritte nützlich und sollten deshalb notiert werden.

Die Risikoeinstufung liefert eine Übersicht über das Ausmaß der Risiken, die sich aus den Gefährdungen für das jeweilige Zielobjekt ergeben. Dabei werden die geplanten oder bereits umgesetzten Sicherheitsmaßnahmen berücksichtigt. Die Behandlung dieser Risiken ist Gegenstand des nächsten Abschnitts.

Beispiel (Auszug):

Bei der Beispielfirma RECPLAST GmbH wurde anhand der Gefährdungsübersicht eine Risikoeinstufung für

- den Virtualisierungsserver S1 (für die Gefährdungen G 0.15 *Abhören* und G 0.25 *Ausfall von Geräten oder Systemen*) sowie
- das Datenbankmanagementsystem A1 (für die Gefährdungen G *0.28 Software-Schwachstellen oder -Fehler* und Gefährdung G 0.32 *Missbrauch von Berechtigungen*)

durchgeführt. Das Ergebnis kann den nachfolgenden Tabellen entnommen werden.

Virtualisierungsserver S1 Vertraulichkeit: hoch Integrität: hoch Verfügbarkeit: hoch		
Gefährdung G 0.15 *Abhören (hier Live-Migration)*	Beeinträchtigte Grundwerte: Vertraulichkeit	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: selten	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: mittel
Beschreibung: Um den Virtualisierungsserver S1 warten zu können, werden alle virtuellen Maschinen (VMs), die darauf ausgeführt werden, auf den Virtualisierungsserver S6 verschoben (Live-Migration). Dabei werden aktuelle Speicherinhalte der VMs von S1 zu S6 übertragen. Aus Performancegründen ist darauf verzichtet worden, die Informationen zu verschlüsseln, so dass der Datenstrom grundsätzlich mitgelesen werden kann. Auch der Datenstrom vom Virtualisierungsserver S1 zu den angeschlossen zentralen Speichersystemen ist unverschlüsselt. Hierdurch können vertrauliche Informationen mitgeschnitten werden. **Bewertung:** Um die virtuelle Infrastruktur sicher betreiben zu können, ist auf Netzebene auf eine geeignete		

Segmentierung geachtet worden. Die einzelnen Netzsegmente (z. B. Management-Netz, Netz für die Live-Migration oder Storage-Netz) sind voneinander getrennt und so konfiguriert worden, dass diese von außen nicht zugänglich sind. Auf das Live-Migration-Netz dürfen nur befugte Administratoren zugreifen. Die Administration der virtuellen Infrastruktur ist in die zentrale Rechteverwaltung des Informationsverbunds eingebunden.

Da nur befugte Administratoren auf das Live-Migration-Netz zugreifen dürfen, können die Speicherinhalte der übertragenen VMs nur von ihnen mitgelesen werden. Den Administratoren wird jedoch vertraut, so dass die Wahrscheinlichkeit für das Abhören als "selten" eingeschätzt wird. Die Auswirkungen werden jedoch aufgrund der Vertraulichkeit der übertragenen Inhalte mit "beträchtlich" eingeschätzt, wodurch sich ein mittleres Risiko ergibt.

Datenbank A1 Vertraulichkeit: hoch Integrität: hoch Verfügbarkeit: hoch		
Gefährdung G 0.28 *Software-Schwachstellen oder -Fehler*	Beeinträchtigte Grundwerte: Vertraulichkeit, Integrität, Verfügbarkeit	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: hoch

Beschreibung:

Um Arbeitszeiten der Mitarbeiter zu erfassen, verwendet die RECPLAST GmbH eine Softwarelösung, die als Webanwendung implementiert ist. Auf die Webanwendung haben alle Mitarbeiter Zugriff und können ihre geleisteten Arbeitsstunden selbstständig eintragen. Die eingetragenen Arbeitsstunden werden von den Abteilungsleitern geprüft und freigegeben. Zusätzlich werden den Mitarbeitern über die Webanwendung am Monatsende die Gehaltsabrechnungen bereitgestellt. Für die Datenhaltung nutzt die Anwendung eine Datenbank, die im Datenbankmanagementsystem (DBMS) betrieben wird.

Die Webanwendung beinhaltet in der eingesetzten Version eine bekannte SQL-Injection-Schwachstelle, die mit vergleichsweise wenig Aufwand ausgenutzt werden kann. Für die Webanwendung sind keine Updates mehr verfügbar, da der Hersteller der Softwarelösung insolvent gegangen ist.

Bewertung:

Auf dem Datenbankmanagementsystem sind alle Berechtigungen so restriktiv wie möglich vergeben, um zu verhindern, dass die Sicherheitslücke einer Anwendung Auswirkungen auf die Datenbanken weiterer Anwendungen hat. Die Auswirkungen der SQL-Injection-Schwachstelle der Webanwendung bleiben also auf die Daten der Webanwendung selbst beschränkt.

Da die SQL-Injection-Schwachstelle der Webanwendung öffentlich bekannt ist und relativ leicht ausgenutzt werden kann, wird die Wahrscheinlichkeit auf "häufig" eingeschätzt. Wird die Lücke erfolgreich ausgenutzt, hat dies Auswirkungen auf die Vertraulichkeit und Integrität der eingegebenen Arbeitsstunden, der Freigabe der Arbeitsstunden und der Gehaltsabrechnungen. Die Auswirkungen werden daher auf "beträchtlich" eingeschätzt. Hierdurch ergibt sich ein hohes Risiko.

Hinweis: Da oftmals sehr viele Zielobjekte und sehr viele Gefährdungen bearbeitet werden müssen, ist der Fließtext bei der Beschreibung und Bewertung einer Gefährdung optional und dient in den obigen Beispielen nur dazu, das Ergebnis der Bewertung nachvollziehbar darzustellen. Bei den in der Tabelle erwähnten Maßnahmen handelt es sich in der Regel um Maßnahmen, die aus den Basis- und Standard-Anforderungen des IT-Grundschutz-Kompendiums abgeleitet worden sind. Die

nachfolgende Darstellung (Bewertung der Gefährdungen G 0.25 *Ausfall von Geräten oder Systemen*, G 0.32 *Missbrauch von Berechtigungen* etc.) ist bei Risikobewertungen vollkommen ausreichend.

Virtualisierungsserver S1 Vertraulichkeit: hoch Integrität: hoch Verfügbarkeit: hoch		
Gefährdung G 0.25 *Ausfall von Geräten oder Systemen* (hier Ausfall des zentralen Verwaltungsservers)	Beeinträchtigte Grundwerte: Verfügbarkeit	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: mittel	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: mittel

Datenbank A1 Vertraulichkeit: hoch Integrität: hoch Verfügbarkeit: hoch		
Gefährdung G 0.32 *Missbrauch von Berechtigungen*	Beeinträchtigte Grundwerte: Vertraulichkeit, Integrität, Verfügbarkeit	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: selten	Auswirkungen ohne zusätzliche Maßnahmen: existenzbedrohend	Risiko ohne zusätzliche Maßnahmen: mittel

Bei dem fiktiven Unternehmen MUSTERENERGIE GmbH wurde für das Zielobjekt Smart Meter Gateway Administration Zx eine Risikoeinstufung (für die Gefährdungen G 0.18 *Fehlplanung oder fehlende Anpassungen* und G 0.32 *Missbrauch von Berechtigungen*) durchgeführt. Das Ergebnis kann der nachfolgenden Tabelle entnommen werden.

Smart Meter Gateway Administration Zx Vertraulichkeit: hoch Integrität: hoch Verfügbarkeit: hoch		
Gefährdung G 0.18 *Fehlplanung oder fehlende Anpassung* (hier: Fehlende oder unzureichende Netzsegmentierung)	Beeinträchtigte Grundwerte: Verfügbarkeit, Vertraulichkeit, Integrität	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: hoch

Gefährdung G 0.32 *Missbrauch von Berechtigungen*	Beeinträchtigte Grundwerte: Verfügbarkeit, Vertraulichkeit, Integrität	
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: häufig	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: hoch
usw.		

6 Behandlung von Risiken

6.1 Risikobehandlungsoptionen

Wie bereits in Kapitel 5 dargestellt, sind je nach Risikoappetit einer Institution unterschiedliche Risikoakzeptanzkriterien möglich. Im Folgenden wird davon ausgegangen, dass eine Institution "geringe" Risiken grundsätzlich akzeptiert, "mittlere", "hohe" und "sehr hohe" Risiken jedoch nur in Ausnahmefällen.

In der Praxis ergeben sich im Rahmen der Risikoeinstufung meist mehrere Gefährdungen, aus denen sich Risiken in den Stufen "mittel", "hoch" oder "sehr hoch" ergeben.

Es muss entschieden werden, wie mit diesen *verbleibenden Risiken* umgegangen wird. Es müssen also geeignete Risikobehandlungsoptionen ausgewählt werden. Risiken können

- vermieden werden, beispielsweise indem die Risikoursache ausgeschlossen wird,
- reduziert werden, indem die Rahmenbedingungen, die zur Risikoeinstufung beigetragen haben, modifiziert werden,
- transferiert werden, indem die Risiken mit anderen Parteien geteilt werden,
- akzeptiert werden, beispielsweise weil die mit dem Risiko einhergehenden Chancen wahrgenommen werden sollen.

Im Folgenden werden die Risikobehandlungsoptionen Vermeidung, Reduktion und Transfer betrachtet. Aufbauend darauf muss eine Institution Risikoakzeptanzkriterien festlegen und die Risikobehandlung darauf abbilden. Bei der Entscheidung, wie mit den identifizierten Risiken umgegangen wird, muss auf jeden Fall die Leitungsebene beteiligt werden, da sich aus der Entscheidung unter Umständen erhebliche Schäden ergeben oder zusätzliche Kosten entstehen können.

Für jede Gefährdung in der vervollständigten Gefährdungsübersicht mit Risikokategorie "mittel", "hoch" oder "sehr hoch" müssen folgende Fragen beantwortet werden:

A. Risiko-Vermeidung: Ist es sinnvoll, das Risiko durch eine Umstrukturierung des Geschäftsprozesses oder des Informationsverbunds zu vermeiden?

Gründe für diesen Ansatz können beispielsweise sein:

- Alle wirksamen Gegenmaßnahmen sind mit hohem Aufwand verbunden und damit sehr teuer, die verbleibende Gefährdung kann aber trotzdem nicht hingenommen werden.
- Die Umstrukturierung bietet sich ohnehin aus anderen Gründen an, zum Beispiel zur Kostensenkung.
- Es kann einfacher und eleganter sein, die vorhandenen Abläufe zu ändern, als sie durch Hinzufügen von Sicherheitsmaßnahmen komplexer zu machen.
- Alle wirksamen Gegenmaßnahmen würden erhebliche Einschränkungen für die Funktion oder den Komfort des Systems mit sich bringen.

B. Risiko-Reduktion (Risiko-Modifikation): Ist es sinnvoll und möglich, das Risiko durch weitere Sicherheitsmaßnahmen zu reduzieren?

Das Risiko durch die verbleibende Gefährdung kann möglicherweise gesenkt werden, indem eine oder mehrere ergänzende Sicherheitsmaßnahmen erarbeitet und umgesetzt werden, die der Gefährdung entgegenwirken. Als Informationsquellen über ergänzende Sicherheitsmaßnahmen kommen beispielsweise in Frage:

- die Dokumentation und der Service des Herstellers, wenn es sich bei dem betroffenen Zielobjekt um ein Produkt handelt,

- Standards und "Best Practices", wie sie beispielsweise von Gremien im Bereich Informationssicherheit erarbeitet werden,
- andere Veröffentlichungen und Dienstleistungen, die beispielsweise im Internet oder von spezialisierten Unternehmen angeboten werden,
- Erfahrungen, die innerhalb der eigenen Institution oder bei Kooperationspartnern gewonnen wurden.

Der hypothetische Aufwand und mögliche Kosten für gegebenenfalls erforderliche Sicherheitsmaßnahmen und Informationen über bereits vorhandene Sicherheitsmechanismen sind wichtige Entscheidungshilfen.

C. Risiko-Transfer (Risiko-Teilung): Ist es sinnvoll, das Risiko an eine andere Institution zu übertragen, beispielsweise durch den Abschluss eines Versicherungsvertrags oder durch Outsourcing?

Gründe für diesen Ansatz können beispielsweise sein:

- Die möglichen Schäden sind rein finanzieller Art.
- Es ist ohnehin aus anderen Gründen geplant, Teile der Geschäftsprozesse auszulagern.
- Der Vertragspartner ist aus wirtschaftlichen oder technischen Gründen besser in der Lage, mit dem Risiko umzugehen.

Wenn im Rahmen der Risikobehandlung zusätzliche Sicherheitsanforderungen identifiziert werden, muss die Risikoeinstufung (siehe nachfolgende Beispiele) für die betroffenen Zielobjekte entsprechend angepasst werden. Zu beachten ist dabei, dass neue Anforderungen unter Umständen nicht nur Auswirkungen auf das jeweils analysierte Zielobjekt haben, sondern auch auf andere Zielobjekte. Die zusätzlichen Anforderungen und die daraus resultierenden Sicherheitsmaßnahmen werden im Sicherheitskonzept dokumentiert.

Wenn im Rahmen der Risikobehandlung Änderungen an den Geschäftsprozessen oder am Informationsverbund vorgenommen wurden, etwa durch Risiko-Vermeidung oder Risiko-Transfer, müssen diese insgesamt im Sicherheitskonzept berücksichtigt werden. Dies betrifft im Allgemeinen auch Arbeitsschritte, die in der IT-Grundschutz-Vorgehensweise gemäß BSI-Standard 200-2 dargestellt sind, beginnend bei der Strukturanalyse. Selbstverständlich kann dabei aber auf die bisher erarbeiteten Informationen und Dokumente zurückgegriffen werden.

Beim Risiko-Transfer ist die sachgerechte Vertragsgestaltung einer der wichtigsten Aspekte. Besonders bei Outsourcing-Vorhaben sollte hierzu auf juristischen Sachverstand zurückgegriffen werden. Die Entscheidung wird von der Leitungsebene getroffen und nachvollziehbar dokumentiert.

D. Risiko-Akzeptanz: Können die Risiken auf Basis einer nachvollziehbaren Faktenlage akzeptiert werden?

Die Schritte Risikoeinstufung und Risikobehandlung werden so lange durchlaufen, bis die Risikoakzeptanzkriterien der Institution erreicht sind und das verbleibende Risiko ("Restrisiko") somit im Einklang mit den Zielen und Vorgaben der Institution steht.

Das Restrisiko muss anschließend der Leitungsebene zur Zustimmung vorgelegt werden ("**Risiko-Akzeptanz**"). Damit wird nachvollziehbar dokumentiert, dass die Institution sich des Restrisikos bewusst ist. Idealerweise akzeptiert eine Institution nur Risiken der Stufe "gering". In der Praxis ist dies aber nicht immer zweckmäßig. Gründe, auch höhere Risiken zu akzeptieren, können beispielsweise sein:

- Die entsprechende Gefährdung führt nur unter ganz speziellen Voraussetzungen zu einem Schaden.
- Gegen die entsprechende Gefährdung sind derzeit keine wirksamen Gegenmaßnahmen bekannt und sie lässt sich in der Praxis auch kaum vermeiden.

- Aufwand und Kosten für wirksame Gegenmaßnahmen überschreiten den zu schützenden Wert.

Hinweis:

Auch diejenigen IT-Grundschutz-Anforderungen, die im IT-Grundschutz-Kompendium als *Anforderungen bei erhöhtem Schutzbedarf* aufgeführt sind, sowie die zugehörigen Maßnahmen, können als Anhaltspunkte für weiterführende Sicherheitsmaßnahmen im Rahmen einer Risikoanalyse herangezogen werden. Dabei handelt es sich um Beispiele, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und in der Praxis häufig angewandt werden. Zu beachten ist jedoch, dass Anforderungen bei erhöhtem Schutzbedarf grundsätzlich empfehlenswert sind, aber auch bei hohen Sicherheitsanforderungen nicht automatisch verbindlich werden. Somit müssen sie auch nicht zwingend in eine Risikoanalyse einbezogen werden.

6.2 Risiken unter Beobachtung

Bei der Risikoanalyse können unter Umständen Gefährdungen identifiziert werden, aus denen Risiken resultieren, die zwar derzeit akzeptabel sind, in Zukunft jedoch voraussichtlich steigen werden. Dies bedeutet, dass sich in der weiteren Entwicklung ein Handlungsbedarf ergeben könnte. In solchen Fällen ist es sinnvoll und üblich, bereits im Vorfeld ergänzende Sicherheitsmaßnahmen zu erarbeiten und vorzubereiten, die in Betrieb genommen werden können, sobald die Risiken inakzeptabel werden.

Diese ergänzenden Sicherheitsmaßnahmen sind zu dokumentieren und vorzumerken. Die Risiken werden beobachtet und sobald sie nicht mehr akzeptabel sind, werden die vorgemerkten ergänzenden Sicherheitsmaßnahmen überprüft, gegebenenfalls aktualisiert und in das Sicherheitskonzept übernommen. Die Risikoeinstufung wird gemäß Kapitel 5 entsprechend angepasst. Nachdem die Risikobehandlung für die verbleibenden Risiken abgeschlossen ist und die Restrisiken von der Leitungsebene akzeptiert wurden, kann das Sicherheitskonzept für den betrachteten Informationsverbund fertig gestellt werden.

Generell sollten jedoch alle Risiken beobachtet werden, also nicht nur solche, die in Zukunft voraussichtlich steigen werden. Um die Beobachtung der Risiken und Anpassung der Maßnahmen bzw. Handlungsalternativen zu dokumentieren, ist es in Praxis üblich hierfür Risikoregister oder Risikoverzeichnisse anzulegen.

Für benutzerdefinierte Bausteine müssen die Gefährdungen in regelmäßigen Zeitabständen überprüft und neu bewertet werden. Da die Zielobjekte, die mit benutzerdefinierten Bausteinen abgedeckt werden, den normalen Anwendungsfall des IT-Grundschutz-Kompendiums überschreiten, müssen die hier beschriebenen Aktivitäten zur Beobachtung von Risiken in jeden Fall berücksichtigt werden.

Beispiel (Auszug):

Für die in Kapitel 5 mit Risikokategorie "mittel" oder "hoch" identifizierten Gefährdungen wurden folgende Entscheidungen getroffen:

Virtualisierungsserver S1 Vertraulichkeit: hoch Integrität: hoch Verfügbarkeit: hoch		
Gefährdung	Risikokategorie	Risikobehandlungsoption
G 0.15 *Abhören* (hier Live-Migration)	mittel	D: Risiko-Akzeptanz (Risiko-Übernahme ohne zusätzliche Maßnahmen) Auf das Live-Migrations-Netz dürfen nur befugte Administratoren zugreifen. Diesen wird vertraut. Das bestehende Restrisiko wird von der RECPLAST als vertretbar eingeschätzt

		und übernommen.
	mittel mit ergänzender Maßnahme: gering	

Datenbank A1 Vertraulichkeit: hoch Integrität: hoch Verfügbarkeit: hoch		
Gefährdung	Risikokategorie	Risikobehandlungsoption
	hoch mit ergänzender Maßnahme: gering	

Datenbank A1 Vertraulichkeit: hoch Integrität: hoch Verfügbarkeit: hoch		
Gefährdung	Risikokategorie	Risikobehandlungsoption
	mittel	

Berechtigungen	mit ergänzender Maßnahme: gering	Ergänzende Sicherheitsmaßnahme: Um das bestehende Risiko zu reduzieren, wird ein zusätzliches Modul des Datenbankmanagementsystems beschafft, mit dem administrative Zugriffe auf kritische Daten in Datenbanken verhindert werden. Zudem werden Aktionen von Administratorkennungen sicher protokolliert und ausgewertet, so dass versuchte Verstöße frühzeitig erkannt werden können.

Smart Meter Gateway Administration Zx Vertraulichkeit: hoch Integrität: hoch Verfügbarkeit: hoch		
Gefährdung	Risikokategorie	Risikobehandlungsoption
	hoch mit ergänzender Maßnahme: gering	
	hoch mit ergänzender Maßnahme: gering	
usw.		

7 Konsolidierung des Sicherheitskonzepts

Falls bei der Behandlung von verbleibenden Gefährdungen ergänzende Maßnahmen zu den bereits im Sicherheitskonzept beschriebenen Sicherheitsmaßnahmen hinzugefügt wurden, muss das Sicherheitskonzept anschließend konsolidiert werden. Konkret bedeutet dies, dass die Sicherheitsmaßnahmen für jedes Zielobjekt anhand folgender Kriterien überprüft werden:

Eignung der Sicherheitsmaßnahmen zur Abwehr der Gefährdungen

- Werden alle Aspekte der relevanten Gefährdungen vollständig abgedeckt?
- Sind die getroffenen Gegenmaßnahmen im Einklang mit den Sicherheitszielen?

Zusammenwirken der Sicherheitsmaßnahmen

- Unterstützen sich die Maßnahmen bei der Abwehr der relevanten Gefährdungen?
- Ergibt sich durch das Zusammenwirken der Maßnahmen ein wirksames Ganzes?
- Stehen die Maßnahmen nicht im Widerspruch zueinander?

Benutzerfreundlichkeit der Sicherheitsmaßnahmen

- Sind die getroffenen Maßnahmen tolerant gegenüber Bedienungs- und Betriebsfehlern?
- Sind die getroffenen Maßnahmen für die Mitarbeiter und andere Betroffene transparent?
- Ist für die Betroffenen ersichtlich, wenn eine Maßnahme ausfällt?
- Können die Betroffenen die Maßnahme nicht zu leicht umgehen?

Angemessenheit / Qualitätssicherung der Sicherheitsmaßnahmen

- Sind die getroffenen Maßnahmen für die jeweiligen Gefährdungen angemessen?
- Stehen die Kosten und der Aufwand für die Umsetzung in einem sachgerechten Verhältnis zum Schutzbedarf der betroffenen Zielobjekte?

Auf dieser Grundlage sollte das Sicherheitskonzept bereinigt und konsolidiert werden:

- Ungeeignete Sicherheitsmaßnahmen sollten verworfen und nach eingehender Analyse durch wirksame Maßnahmen ersetzt werden.
- Widersprüche oder Inkonsistenzen bei den Sicherheitsmaßnahmen sollten aufgelöst und durch einheitliche und aufeinander abgestimmte Mechanismen ersetzt werden.
- Sicherheitsmaßnahmen, die von den Betroffenen nicht akzeptiert werden, sind wirkungslos. Es sollten praktikable Lösungen erarbeitet werden, die die Betroffenen möglichst wenig einschränken oder behindern.
- Zu aufwändige oder zu teure Sicherheitsmaßnahmen sollten entweder überarbeitet oder verworfen und durch angemessene Schutzmaßnahmen ersetzt werden. Auf der anderen Seite gefährden zu schwache Maßnahmen die Informationssicherheit. Auch sie sollten überarbeitet oder ersetzt werden.

Integration der Inhalte

- Bei Zielobjekten, die bereits im IT-Grundschutz-Kompendium enthalten sind, kann es sich als sinnvoll erweisen, bestehende Bausteine um aus der Risikoeinstufung ermittelte Anforderungen zu ergänzen.
- Bei Zielobjekten, die nicht hinreichend mit dem bestehenden IT-Grundschutz abgebildet werden können, kann überlegt werden, die neu gefundenen Gefährdungen und Anforderungen (siehe Beispiele zu Smart Meter Gateway Administration, Kapitel 4 und 5) in einem benutzerdefinierten Baustein zusammenzufassen.

Beispiel (Auszug):

Bei der Konsolidierung des Sicherheitskonzepts für die RECPLAST GmbH wurde unter anderem Folgendes festgestellt:

- Vor zwei Jahren wurde entschieden, dass der Einsatz von Verschlüsselung zur Netzkommunikation entbehrlich ist. Eine gemeinsame Projektgruppe mit dem Auftraggeber ist zu dem Ergebnis gekommen, dass diese Entscheidung nicht mehr dem Stand der Technik entspricht. Die Vorgaben zur Konfiguration der Router werden deshalb kurzfristig überarbeitet und an die aktuellen Bedürfnisse angepasst.

  Sowohl der Client C1 als auch der Switch N3 werden im Fertigungsbereich eingesetzt. Im Rahmen der Risikoanalyse wurde festgestellt, dass die größten Gefahren für C1 von Luftverunreinigungen, Spritzwasser und Vibrationen ausgehen. Im Rahmen eines Brainstormings ist deshalb beschlossen worden, anstelle eines handelsüblichen PCs einen Industrie-PC einzusetzen, der besonders gegen physische Gefahren geschützt ist. Der Industrie-PC muss für den Einbau in Standard-19-Zoll-Schränke geeignet sein. Darüber hinaus muss er über ein integriertes oder ausklappbares Display sowie einen leicht auswechselbaren Luftfilter verfügen und gegen Spritzwasser und Vibrationen schützen.

- Oben genannte Anforderungen tragen den besonderen infrastrukturellen Rahmenbedingungen des Clients C1 Rechnung. Im Fertigungsbereich wird außer diesem Client weitere Informationstechnik betrieben, die zwar nicht Gegenstand der Risikoanalyse ist, die aber dennoch angemessen geschützt werden muss. Das Unternehmen nimmt die Erfüllung obiger Anforderungen zum Anlass, eine Richtlinie für den sicheren Betrieb von Informationstechnik im Fertigungsbereich zu erarbeiten.

- usw.

Beispiel (Auszug):

Bei der Konsolidierung des Sicherheitskonzepts für die Administration des Smart Meter Gateways ist entschieden worden, die im Rahmen der Risikoeinstufung und -behandlung ermittelten Gefährdungen

- G 0.18 *Fehlplanung oder fehlende Anpassungen*,
- G 0.30 *Unberechtigte Nutzung oder Administration von Geräten und Systemen*,
- G 0.43 *Einspielen von Nachrichten*
- usw.

und die Sicherheitsanforderungen und Maßnahmen

- Geeignete Netzsegmentierung
- Einsatz eines angemessenen Rollen- und Rechtekonzepts
- usw.

in einem benutzerdefinierten Baustein zusammenzufassen.

8 Rückführung in den Sicherheitsprozess

Nach der Konsolidierung des Sicherheitskonzepts kann der Sicherheitsprozess, wie er im BSI-Standard 200-2 *IT-Grundschutz-Methodik* (siehe [BSI2]) beschrieben ist, fortgesetzt werden. Das ergänzte Sicherheitskonzept dient somit als Basis für folgende Arbeitsschritte:

- **IT-Grundschutz-Check** (siehe Kapitel 8.4 der IT-Grundschutz-Methodik). Im Rahmen der Vorarbeiten wurde bereits ein IT-Grundschutz-Check für die laut IT-Grundschutz-Modell zu erfüllenden Sicherheitsanforderungen durchgeführt. Da sich bei der Risikoanalyse in der Regel Änderungen am Sicherheitskonzept ergeben, ist anschließend noch der Umsetzungsstatus der neu hinzugekommenen oder geänderten Anforderungen zu prüfen. Gegebenenfalls veraltete Ergebnisse sollten auf den neuesten Stand gebracht werden.
- **Umsetzung der Sicherheitskonzeption** (Kapitel 9 der IT-Grundschutz-Methodik). Die im Sicherheitskonzept für die einzelnen Zielobjekte vorgesehenen Sicherheitsanforderungen müssen erfüllt werden. Hierfür müssen die daraus abgeleiteten Sicherheitsmaßnahmen in die Praxis umgesetzt werden, damit sie wirksam werden können. Dies umfasst unter anderem eine Kosten- und Aufwandsschätzung sowie die Festlegung der Umsetzungsreihenfolge.
- **Überprüfung des Informationssicherheitsprozesses in allen Ebenen** (siehe Kapitel 10.1 der IT-Grundschutz-Methodik). Zur Aufrechterhaltung und kontinuierlichen Verbesserung der Informationssicherheit müssen unter anderem regelmäßig die Erfüllung der Sicherheitsanforderungen und die Eignung der Sicherheitsstrategie überprüft werden. Die Ergebnisse der Überprüfungen fließen in die Fortschreibung des Sicherheitsprozesses ein.
- **Informationsfluss im Informationssicherheitsprozess** (siehe Kapitel 5.2 der IT-Grundschutz-Methodik). Um Nachvollziehbarkeit zu erreichen, muss der Sicherheitsprozess auf allen Ebenen dokumentiert sein. Dazu gehören insbesondere auch klare Regelungen für Meldewege und Informationsflüsse. Die Leitungsebene muss von der Sicherheitsorganisation regelmäßig und in angemessener Form über den Stand der Informationssicherheit informiert werden.
- **ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz** (siehe Kapitel 11 der IT-Grundschutz-Methodik). In vielen Fällen ist es wünschenswert, den Stellenwert der Informationssicherheit und die erfolgreiche Umsetzung des IT-Grundschutzes in einer Behörde bzw. einem Unternehmen transparent zu machen. Hierfür bietet sich eine *ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz* an.

9 Anhang

9.1 Risikoappetit (Risikobereitschaft)

Risikoappetit bezeichnet die durch kulturelle, interne, externe oder wirtschaftliche Einflüsse entstandene Neigung einer Institution, wie sie Risiken einschätzt, bewertet und mit ihnen umgeht.

Die Neigung innerhalb einer Institution, Risiken einzugehen, wird durch eine Vielzahl von Faktoren beeinflusst, so dass eine quantitative Einstufung des Risikoappetits recht komplex werden kann. Ein Ziel dieses Kapitels ist es, die Komplexität zu verringern und eine beherrschbare Zahl von Risikoneigungstypen zu definieren, denen Empfehlungen für einen sinnvollen Umgang mit Risiken gegeben werden kann.

9.1.1 Einflussfaktoren

Zu den äußeren Bedingungen, die die Risikoneigung einer Institution beeinflussen, gehören:

- Kulturelle Einflüsse (je nach Land und Mentalität gibt es unterschiedliche Bereitschaften, Risiken einzugehen)
- Interne Faktoren (Organisationskultur, Einstellung des Managements, Risiken als Problem oder Chance zu sehen)

  Konservative Institutionen neigen eher zur Risikovermeidung (z. B. Behörden oder Unternehmen, die um ein besonders seriöses Image bemüht sind). Schnell wachsende Unternehmen sind eher bereit, Risiken zu tragen, wohingegen etablierte Großunternehmen Risiken eher meiden. Bei Großunternehmen ist es manchmal jedoch auch sinnvoll, das Risikomanagement für unterschiedliche Unternehmensbereiche unterschiedlich aufzusetzen, je nachdem ob es sich bei den Bereichen um neue, technologieintensive Bereiche (mit hoher Risikoneigung) oder "Cash Cows" (mit niedriger Risikoneigung) handelt. Großunternehmen haben hier den Vorteil, dass sie Risiken über verschiedene Bereiche streuen können. Daher kann der Risikoappetit in verschiedenen Unternehmensteilen auch unterschiedlich sein. Je klarer Visionen und strategische Ziele der Institution sind, desto direkter ergibt sich daraus auch eine Einstellung zu Risiken.
- Marktumfeld (z. B. konservatives oder innovatives Umfeld)

  Marktumfeld und interne Faktoren stehen in einem engen Zusammenhang. Wer in neue Märkte einsteigt, muss sich auf die dort geltenden Regeln und insbesondere auf Wettbewerb einstellen, auch wenn dies eventuell der Tradition der Institution zuwiderläuft. Es ist sinnvoll, konkurrierende Institutionen zu beobachten und die eigene Handlungsweise (z. B. nach den Regeln der Spieltheorie) danach auszurichten. Die Strategie kann (hier wiederum nach der Kultur innerhalb der Institution) darauf hinauslaufen, an der Spitze des Marktes stehen zu wollen: In diesem Fall wird Bereitschaft gezeigt werden müssen, hohe Risiken einzugehen. Im anderen Fall kann sich die Institution entscheiden, als "Fast Follower" zu agieren. Dies bedeutet, dass sie versucht, der Konkurrenz die Risiken zu überlassen und trotzdem einen attraktiven Marktanteil zu erringen. Bei der Entscheidung, ob eine Institution bestimmte Maßnahmen umsetzt oder nicht, spielt auch häufig eine Rolle, was die Konkurrenz macht (sofern deren Maßnahmen bekannt sind).
- Risikotragfähigkeit (Finanzierung der Institution (Haftung, Kapitaldecke etc.))

  Obwohl Großunternehmen, wie schon erwähnt, eher zur Risikovermeidung neigen, haben sie üblicherweise eine Kapitaldecke, die es zumindest bei Teilbereichen erlaubt, Risiken zu tragen. Kleine Unternehmen, die über eine eher geringe Kapitaldecke verfügen, aber trotzdem aus Gründen des Marktumfeldes signifikante Risiken eingehen müssen, arbeiten aus demselben Grund manchmal mit Risikokapitalgebern zusammen.

9.1.2 Quantifizierung von Risikoneigung

Vereinfacht dargestellt läuft Risikomanagement in folgenden Schritten ab. Präzise Definitionen können z. B. ISO/IEC 31000 (siehe [31000]) oder NIST SP 800-30 (siehe [NIST800-30]) entnommen werden:

- Identifikation von Risiken
- Risikoeinschätzung (Ermittlung von Eintrittshäufigkeit und Schadenshöhe)
- Risikobewertung (Ermittlung der Risikokategorie)
- Bestimmung von Maßnahmen zur Behandlung von Risiken
- Vergleich der Kosten jeder Maßnahme mit zu erwartenden Schäden und Entscheidung für oder gegen die Umsetzung der Maßnahme
- Restrisikobetrachtung: Festlegung von Handlungsoptionen
- Abgleich mit Chancen (erwartete Einnahmen und Nutzen des Geschäftsfeldes)
- Verfolgung der Risiken und Anpassung der Maßnahmen bzw. Handlungsoptionen im laufenden Betrieb

In mehreren dieser Schritte kann sich die Risikoneigung einer Institution widerspiegeln.

Kriterien für Risikoneigung

Beim Versuch, Kriterien für die Risikoneigung festzulegen, ergeben sich mehrere mögliche Ansätze. Es folgen einige Beispiele:

- Höchstmögliches akzeptables Risiko
- Höchstmögliche akzeptable Eintrittshäufigkeit für Risiken
- Akzeptanz von Risiken bei gleichzeitig hohen Marktchancen
- Akzeptanz von Unvorhersagbarkeit (z. B. wenn sich Risiken nur sehr schwer einer Häufigkeit oder Schadenssumme zuordnen lassen)
- Auswahl von Behandlungsalternativen ab einem bestimmten Restrisiko

Nicht immer lassen sich Einstellungen gegenüber Risiken rational begründen. Ein Beispiel wäre die pauschale Abneigung einer Institution, Risiken mit hoher Eintrittshäufigkeit einzugehen, denn wenn mit diesen Risiken keine hohen Schäden einhergingen, müssten sie nicht unbedingt vermieden werden. Eine derartige Entscheidung könnte aber trotzdem intuitiv gefällt werden, wenn die Institution sich bei der Bestimmung der Schadenshöhe nicht ausreichend sicher ist. Ein analoges Argument träfe bezüglich der Einstellung gegenüber einer maximal akzeptierten Schadenssumme zu. Unpräzises Datenmaterial führt dazu, dass sich Institutionen in der einen oder anderen Weise entscheiden müssen. Dabei wird die Entscheidung von der Risikoneigung stark beeinflusst.

Optimale Strategie und Unsicherheit

Wenn sich alle Parameter, die in das Risikomanagement eingehen, exakt bestimmen ließen, wäre auch ein optimaler Umgang mit diesen Risiken ermittelbar. Diese Parameter sind beispielsweise die Eintrittshäufigkeiten und Schadenssummen (vor und nach Behandlung durch Maßnahmen), die Kosten von Maßnahmen, die Kosten von Behandlungsalternativen und die erwarteten Chancen, also z. B. Einnahmen aus einem Geschäft.

Risiken müssen immer gegen Chancen abgewogen werden. Typisch wäre beispielsweise bei einem Geschäftsfeld, mit dem Risiken verbunden sind, dass risikoscheue Institutionen das Risiko vermeiden und gleichzeitig die entsprechende Chance verpassen, während weniger risikoscheue Institutionen das Risiko eingehen, aber damit gleichzeitig die Chance wahrnehmen.

Wenn sich die oben erwähnten Parameter alle exakt ermitteln ließen, könnte ein präziser Erwartungswert für die erzielten Gewinne oder Verluste der Institution ermittelt werden, abhängig davon, ob das Risiko eingegangen wird oder nicht. In diesem Falle gäbe es eine optimale Strategie für die Institution und die Frage der Risikoneigung würde keine Rolle mehr spielen.

Daran wird deutlich, dass die Risikoneigung deswegen bedeutsam ist, weil die Eingangsdaten für das Risikomanagement mit Unsicherheit behaftet sind. Die Frage ist, wie man die Unsicherheiten bewertet und wie die Institution für einen hohen Schadensfall gerüstet ist.

Mögliche Maßzahlen

Unabhängig von eher intuitiv begründeten Risikoneigungen, wie sie oben beschrieben wurden, soll versucht werden, Maßzahlen für die Risikoneigung zu ermitteln. Dabei wird von den Schritten ausgegangen, die oben beim grundsätzlichen Vorgehen beim Risikomanagement beschrieben wurden, und es soll eine rationale Vorgehensweise bei der Beurteilung der Risiken angestrebt werden.

Die einfachste Maßzahl orientiert sich am Erwartungswert für die Schadenshöhe, definiert als Produkt aus Eintrittshäufigkeit für das Risiko und der Schadenshöhe. Risiken werden oft als Matrix dargestellt, bei der auf der einen Achse die Eintrittshäufigkeit und auf der anderen die Schadenhöhe dargestellt wird. Die hohen Risiken befinden sich in der Matrix in einem rot eingefärbten Bereich. "Hoher Risikoappetit" könnte also im einfachsten Falle als Bereitschaft definiert werden, auch Risiken in diesem Bereich zu akzeptieren. "Niedriger Risikoappetit" hieße Vermeidung, also möglicherweise gleichzeitig Verzicht auf eine Einnahmechance.

Abbildung 4 zeigt eine beispielhafte Risikomatrix mit definierten Risikokategorien.

Um die Schwellwerte festzulegen, mittels derer die Eintrittshäufigkeiten und Auswirkungen als "hoch" eingestuft werden, orientieren sich Institutionen typischerweise an ihren finanziellen Kennzahlen. Die Leitungsebene entscheidet, welche Schwellwerte sie als "hoch" einstuft. Die Schwelle könnte sich an den finanziellen Rücklagen orientieren, aber auch am Umsatz der Institution. So kann die Schwelle als ein bestimmter Prozentsatz des Umsatzes festgelegt werden. Sie kann sich aber auch daran orientieren, ob die Institution bei Eintritt eines bestimmten Risikos noch liquide wäre. Je nach Höhe des Risikos müssen Entscheidungen normalerweise von verschiedenen Führungsebenen genehmigt werden, hohe Risiken sollten nicht ohne Erlaubnis des Top-Managements eingegangen werden.

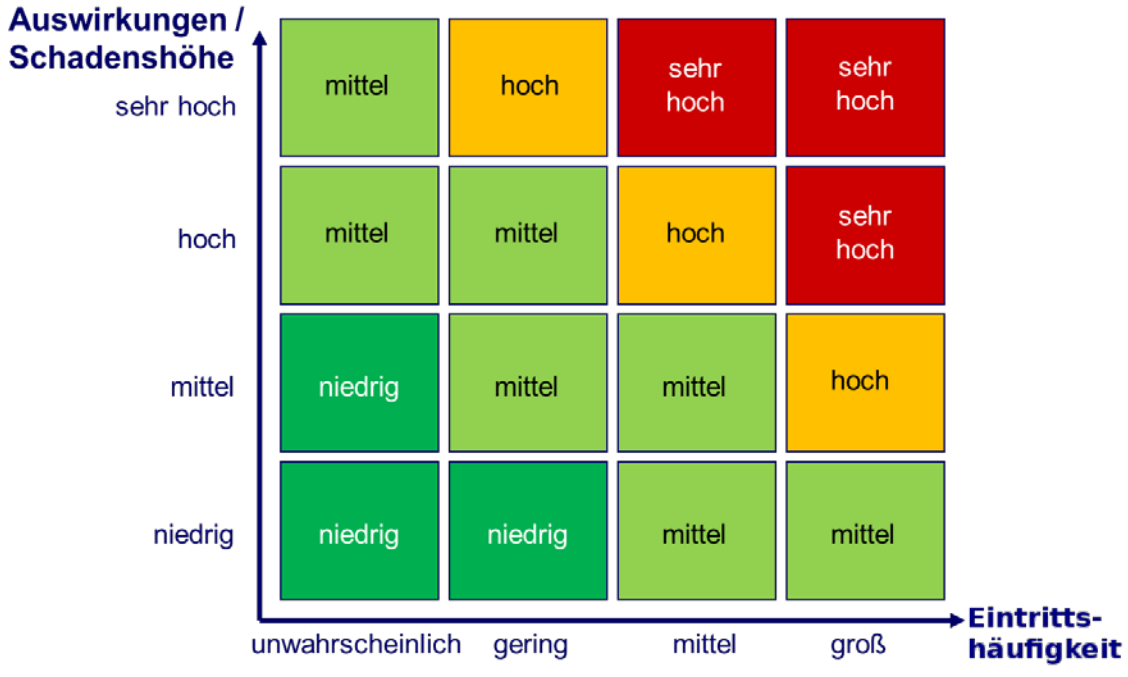


Abbildung 4: Beispielhafte Risikomatrix mit Risikokategorien

Wenn also Risiken eingeschätzt und in die oben dargestellte Risikomatrix eingetragen werden, ergibt sich eine Darstellung wie in Abbildung 5, in der sechs verschiedene Risiken ermittelt wurden und als Kreise mit Nummern eingetragen sind. Hier würde eine Institution mit hohem Risikoappetit (obere der zwei schwarzen Linien) die Risiken 1 und 3 unterhalb der Linie noch tragen, während eine Institution mit niedrigem Risikoappetit nur die Risiken 4, 5 und 6 tragen würde (untere Linie). Risiko 2 würde in diesem Fall keine Institution tragen.

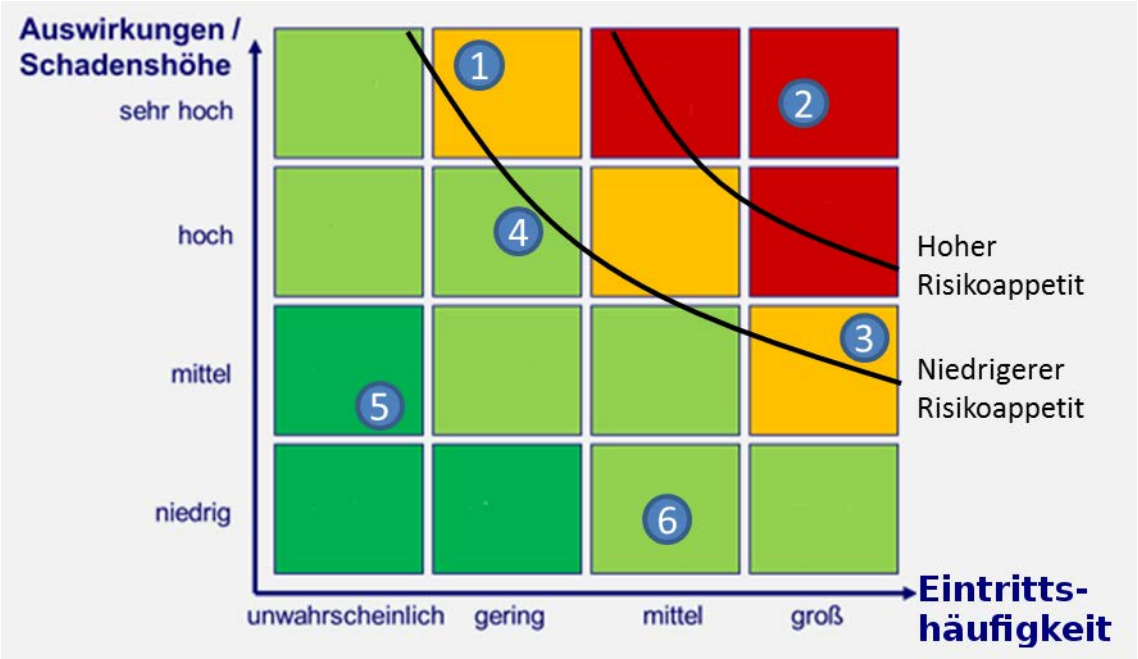


Abbildung 5: Risikomatrix mit eingetragenen Risiken

Wie oben schon erwähnt, gäbe es aber auch für Institutionen mit geringem Risikoappetit keinen Grund, auf Chancen zu verzichten, wenn verlässliche Daten Einnahmen erwarten ließen, die die Kosten durch eingetretene Risiken überträfen. Einzig und allein die Unsicherheiten bei den erhobenen Daten sind der Grund dafür, dass Institutionen mit geringerem Risikoappetit in derartigen Situationen zur Risikovermeidung neigen.

Eine andere Definition für Risikoappetit besteht in der Akzeptanz von Unsicherheiten bei der Interpretation des Datenmaterials. Gerade bei innovativen Branchen können Institutionen nicht auf viel vorhandenes Datenmaterial bei der Ermittlung von Eintrittshäufigkeit und Schadenshöhe von Risiken zurückgreifen. Unwägbarkeiten kommen bei Risiken im Bereich Informationssicherheit nahezu immer ins Spiel, im Gegensatz zu statistisch gut vorhersagbaren Risiken, wie sie beispielsweise zu Elementarschäden in der Versicherungswirtschaft vorliegen.

Die Unsicherheiten lassen sich in einem Risikodiagramm beispielsweise mit Fehlerbalken darstellen, die die Unsicherheit der Daten repräsentieren. Auch die Längen dieser Fehlerbalken sind bei größerer Unsicherheit nur intuitiv zu ermitteln.

Abbildung 6 zeigt eine Risikomatrix mit Fehlerbalken. Sie sind in diesem Beispiel vertikal ausgerichtet, geben also eine Unsicherheit bei der Schadenshöhe an. Fehlerbalken in horizontaler Ausrichtung wären genauso denkbar. Institutionen mit geringem Risikoappetit würden sich in dieser Darstellung eher am oberen Rande der Werte für die Eintrittshäufigkeit und Schadenshöhe orientieren, Institutionen mit hohem Risikoappetit in der Mitte (nicht am unteren Rande, weil das wiederum hieße, Risiken systematisch zu unterschätzen).

Interessant ist ein Vergleich der Risiken 4 und 5: Eine Institution mit niedriger Risikoneigung würde in dieser Situation vielleicht eher das Risiko 4 als das Risiko 5 akzeptieren, obwohl es einen höheren Erwartungswert für den Schaden trägt. Hier ist die Unsicherheit bei der Schadenshöhe ausschlaggebend, die bei Risiko 5 höher liegt, gekennzeichnet durch den Fehlerbalken, der bei Risiko 5 in größere Schadenshöhen hineinragt als der von Risiko 4.

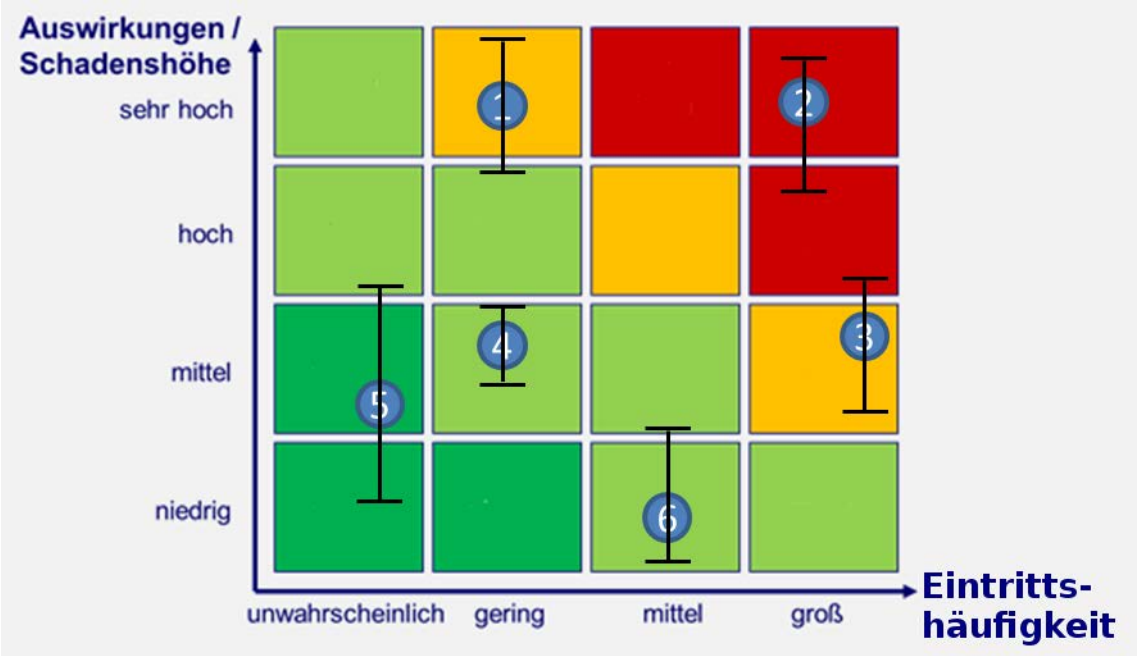


Abbildung 6: Risikomatrix mit Unsicherheiten

Zuletzt gibt es auch noch die Möglichkeit, Risiken in unterschiedliche Kategorien einzuteilen und einen unterschiedlichen Risikoappetit pro Kategorie zu entwickeln. Beispielsweise könnte eine Institution Rufschädigungen scheuen, aber bereit sein, hohe finanzielle Risiken einzugehen. Dadurch ändert sich prinzipiell nichts am Vorgehen, sondern die unterschiedlichen Kategorien werden einfach gesondert voneinander betrachtet.

Risikotypen

In einem einfachen Modell kann man Institutionen je nach ihrem Umgang mit Risiken in verschiedene Typen unterteilen. Eine beispielhafte Unterteilung wäre die folgende:

- "Cowboy " – entspricht einer Institution, die Risiken prinzipiell bereitwillig in Kauf nimmt
- "Risk-Eater " – nimmt hohe Risiken in Kauf, wenn diesen auch hohe Chancen gegenüberstehen
- "Konservativer " – versucht alle Risiken durch Maßnahmen soweit wie möglich zu minimieren

Wenn unter "Cowboy" eine Institution verstanden wird, die Risiken einfach ignoriert, widerspricht das den Prinzipien des Risikomanagements, und verlässliche Angaben über zu erwartende Konsequenzen, also Schäden oder Chancen sind schwer möglich.

Für die folgende Betrachtung soll angenommen werden, dass eine Institution ein professionelles Risikomanagement betreibt. Auch wenn ein professionelles Risikomanagement nicht immer verhindern kann, dass schlechte Entscheidungen getroffen werden, so stellt es dennoch sicher, dass diese bewusst aufgrund vorhandener Analysen getroffen wird. Die Risikoneigung sollte keinen Einfluss darauf haben, ob überhaupt eine Risikoanalyse durchgeführt wird und mit welcher Sorgfalt dies geschieht. Sie kann allerdings Einfluss darauf haben, wieviel Ressourcen die Institution in Risikoanalyse und -behandlung investiert. Dabei sollte es sich jedoch um eine bewusste Entscheidung handeln.

Für den Rest dieses Kapitels werden folgende Kategorien benutzt:

- Konservativer

  Der Konservative scheut Risiken, die sich in der Risiko-Matrix im roten (und eventuell auch gelben) Bereich befinden (siehe Abbildung 4) und meidet diese. Die damit verbundenen Chancen sind ihm zu unsicher, um sich auf die Gefahren einzulassen.

- Risikoaffiner

  Der Risikoaffine sieht stets die Chancen, die mit hohen Risiken verbunden sind. Wenn diese vielversprechend ausfallen – aber auch nur dann – ist er bereit, das Risiko einzugehen. Institutionen, die jedes Risiko eingehen, auch wenn ihnen keine gleichwertigen Chancen gegenüberstehen, handeln selbstzerstörerisch und werden im Folgenden nicht weiter betrachtet.

- Unsicherheitsvermeider

  Der Unsicherheitsvermeider versucht, möglichst verlässliche Daten über seine Risiken zu sammeln. Er neigt eher zur Vermeidung von Risiken, wenn diese sich quantitativ schwer einschätzen lassen, als wenn diese hoch, aber gut kontrollierbar und durch solide Finanzierung oder zu erwartende Einnahmen abgedeckt sind. Im letzteren Punkt unterscheidet er sich vom Konservativen.

9.1.3 Risikoneigung als Eingangsgröße im ISMS

Da die Risikoanalyse ein wichtiger Bestandteil des ISMS ist, sollten die Grundvoraussetzungen dafür vom Management der Institution vorgegeben werden. Die Leitungsebene gibt die Risikoneigung vor. Das Sicherheitsmanagement muss die Risikoneigung kennen und sie entsprechend umsetzen.

Möglicherweise ist sich eine Institution ihrer eigenen Risikoneigung nicht bewusst oder hat ungenaue Vorstellungen von diesem Begriff. In diesem Fall sollte das Management eine Klärung und Entscheidung herbeiführen, gegebenenfalls unter Beratung durch eine Fachkraft (z. B. durch den Informationssicherheitsbeauftragten bzw. ISB oder Risikomanager). Dabei werden die oben genannten Einflussfaktoren berücksichtigt. Die für das Anforderungsmanagement (Corporate Compliance) zuständige Organisationseinheit sollte ebenfalls gehört werden.

Die vom Management vorgegebene Aussage zur Risikoneigung kann zu Beginn der Risikoanalyse präzisiert werden, im Sinne der oben definierten Kategorien oder Maßzahlen. Wichtig ist es, diese Vorgabe einerseits regelmäßig zu überprüfen und an den Zielen der Institution auszurichten, sie aber bei Risikoanalysen und -behandlungen auch konsequent umzusetzen. Zweifelsfälle können auftreten, beispielsweise wenn es bei einem bestimmten Risiko nicht sinnvoll erscheint, die festgelegte Risikoneigung anzuwenden. Solche Ausnahmefälle sollten abgestimmt und dokumentiert werden.

Oben wurde beschrieben, auf welche Aspekte die Risikoneigung Einfluss haben kann. Wenn Entscheidungen getroffen werden, die durch die Risikoneigung mitbeeinflusst wurden, sollte dies dokumentiert werden.

Sobald die Risiken eingeschätzt und bewertet wurden, sollte bereits aufgrund der vorgegebenen Risikoneigung über eine mögliche Behandlung dieser nachgedacht werden, bevor ergänzende Sicherheitsmaßnahmen ermittelt werden. Unter Umständen lohnt sich die Planung von ergänzenden Sicherheitsmaßnahmen nicht. Im entgegengesetzten Fall werden Sicherheitsmaßnahmen geplant und bewertet, um das Risiko zu verringern und anschließend das Restrisiko bewertet. Restrisiken müssen behandelt werden, wenn sie das akzeptierte Risiko übersteigen. Bei der Entscheidung für eine Behandlungsoption geht abermals die Risikoneigung ein.

Bei der Entscheidung, ob ein Risiko selbst getragen oder transferiert werden soll, wird der "Risikoaffine" tendenziell eher zur ersten, die Typen "Konservativer" und "Unsicherheitsvermeider" eher zur zweiten Option neigen, obwohl pauschale Aussagen hier nicht immer zutreffen. Der "Unsicherheitsvermeider" wird gegebenenfalls versuchen, durch die Umsetzung von Maßnahmen unter seiner eigenen Kontrolle die Unsicherheit bei der Risikoeinschätzung zu verringern.

Auch bei den einzelnen Entscheidungen, die bei der Risikoanalyse und -behandlung getroffen werden, empfiehlt es sich, den Einfluss der Risikoneigung auf diese Entscheidungen zu dokumentieren. Bei einer Änderung der Risikoneigung (z. B. durch veränderte Marktbedingungen) lässt sich die Risikoanalyse dann leichter anpassen.

Die Risikoneigung hat zudem Einfluss auf die Aufbauorganisation einer Institution. Ein Beispiel ist die Frage, ob es eine Organisationseinheit für das Risikomanagement gibt und wie diese

zusammengesetzt ist, obwohl diese Entscheidung natürlich von Faktoren wie der Firmengröße mitbestimmt wird.

Generell lautet die Empfehlung: Wer sich zu einer hohen Risikoneigung bekannt hat (Typus "Risikoaffiner"), sollte dem in seinem Risikomanagementprozess und seiner Organisationsstruktur Rechnung tragen. Hohe Risiken verlangen aufmerksame Verfolgung und Kontrolle.

9.1.4 Auswirkung von Gesetzen und Regulatorien

Gesetze und Normen beeinflussen nicht die Risikoneigung einer Institution an sich, aber den Umgang mit Risiken. Die Risiken nehmen durch regulatorischen Druck zu, so dass sich das Verhältnis von Risikoappetit zu den ursprünglichen Risiken verschieben kann. Jede Institution muss Sanktionen aufgrund von rechtlichen oder vertraglichen Verstößen in ihr Risikokalkül mit aufnehmen.

Ein Beispiel für Gesetze, die das Risikomanagement von Unternehmen beeinflussen, sind Datenschutzgesetze. Bei etlichen Unternehmen gab es trotz vorbeugender Maßnahmen Datenschutzpannen. Vor dem Hintergrund dieser Erfahrungen sollte dies beim Risikomanagement berücksichtigt werden. Insbesondere geht es darum, die gemachten Fehler, die zu den Datenschutzverstößen führten, zu lokalisieren und geeignete Maßnahmen abzuleiten und umzusetzen. In Frage kommen beispielsweise Schulungen der Mitarbeiter und Awareness-Kampagnen.

Beispiele für Regularien durch Aufsichtsstellen gibt es viele, beispielsweise im Bankenwesen. Entscheidungen einer Institution, Risiken auf jeden Fall zu tragen, obwohl bei seriöser Betrachtung die Kapitaldecke dafür nicht ausreichen würde, werden durch Vorschriften der Finanzaufsicht unterbunden oder mit entsprechenden Sanktionen belegt.

9.2 Moderation der Risikoanalyse

Für eine Risikoanalyse müssen Fachverantwortliche bzw. Experten für die jeweils betrachteten Zielobjekte mit einbezogen werden. In der Praxis hat es sich bewährt, hierzu besser mehrere kurze als eine lange Sitzung mit allen beteiligten Mitarbeitern durchzuführen. Es sollten Informationssicherheitsbeauftragte, Fachverantwortliche, Administratoren und Benutzer des jeweils betrachteten Zielobjekts und gegebenenfalls auch externe Sachverständige beteiligt werden.

Es sollte ein Moderator benannt werden. Der Arbeitsauftrag an die Teilnehmer sollte klar formuliert sein und die Zeit für die Sitzungen begrenzt werden.

Damit die für die jeweiligen Schritte der Risikoanalyse notwendigen Beschlüsse direkt konsolidiert werden können, z. B. zu Risikoakzeptanz, Kosten und Umsetzbarkeit, sollte (zumindest gegen Ende) ein Vertreter der Leitungsebene anwesend sein.

Das Team sollte nicht zu groß sein (bewährt haben sich 4 bis 8 Personen). Es sollte im Team ausreichend Expertise für alle Aspekte des betrachteten Bereichs vorhanden sein.

- Der Moderator sollte schon an Risikoanalysen teilgenommen haben, so dass er die Vorgehensweise kennt.
- Die Besprechung sollte unter Rahmenbedingungen stattfinden, die ein ungestörtes Arbeiten ermöglichen, da hohe Konzentration erforderlich ist.
- Der Analysebereich sollte klar abgegrenzt werden.
- Es muss ein klarer Maßstab für die Bewertung von Risiken festgelegt werden, damit alle Risiken mit demselben Niveau behandelt werden und die ergriffenen Maßnahmen vergleichbar und nachvollziehbar sind.
- Alle Teilnehmer sollten den groben Rahmen der Risikoanalyse und des betrachteten Bereichs kennen, so dass sie sich vorab Gedanken machen konnten über Gefährdungen, Schadensauswirkungen und Maßnahmen. Dazu gehört auch, dass sie die zum betrachteten Bereich gehörenden Objekte kennen wie auch die zugehörigen Geschäftsprozesse, Hintergründe, Einbettung in die Organisation und die Technik sowie technische Grundlagen.

- Alle Gefährdungen, die Teilnehmern einfallen, sollten auch genannt und diskutiert werden. Es ist Aufgabe des Moderators, dafür zu sorgen, dass bei den Diskussionen die Ergebnisfindung nicht aus den Augen verloren wird.
- Detailfragen, die besondere Expertise erfordern, sollten im Vorfeld vorbereitet werden. Einzelne Punkte können auch im Anschluss geklärt werden.
- Es sollte ein Ergebnisbericht erstellt werden. Da viele potentielle Angriffspunkte diskutiert wurden, sollten die Unterlagen vertraulich behandelt werden.

Für die Durchführung jeder Risikoanalyse sollte es klare zeitliche Vorgaben geben. Erfahrungen zeigen, dass die Resultate umso besser werden, je systematischer und konzentrierter vorgegangen wird, nicht je länger es dauert. Auch eine Risikoanalyse für komplexe Sachverhalte ist normalerweise an einem Tag zu schaffen. Wenn der betrachtete Bereich zu umfangreich ist, sollte er in Teilbereiche aufgeteilt werden. Auch bei einer Risikoanalyse sollte die 80:20-Regel beachtet werden. Da ohnehin nicht jeder mögliche Sachverhalt betrachtet werden kann, sollten immer die am wahrscheinlichsten Gefährdungen und die plausibelsten Lösungen im Vordergrund stehen. Wenn esoterische Gefährdungen diskutiert werden, also solche, die extrem selten und hochgradig unwahrscheinlich sind, ist das ein Zeichen, dass die erforderliche Konzentration nicht mehr gegeben ist.

9.3 Ermittlung zusätzlicher Gefährdungen

Die folgenden Fragestellungen sollten bei der Ermittlung zusätzlicher Gefährdungen berücksichtigt werden:

- Von welchen Ereignissen aus dem Bereich *höhere Gewalt* droht besondere Gefahr für den Informationsverbund?
- Welche *organisatorischen Mängel* müssen vermieden werden, um die Informationssicherheit zu gewährleisten?
- Welche *menschlichen Fehlhandlungen* können die Sicherheit der Informationen besonders beeinträchtigen?
- Welche speziellen Sicherheitsprobleme können beim jeweils betrachteten Zielobjekt durch *technisches Versagen* entstehen?
- Welche besondere Gefahr droht durch vorsätzliche Angriffe von *Außentätern*? Damit sind Personen gemeint, die nicht der eigenen Institution angehören und auch nicht durch besondere Vereinbarungen Zugang zu oder Zugriff auf interne Ressourcen haben.
- Auf welche Weise können *Innentäter* durch vorsätzliche Handlungen den ordnungsgemäßen und sicheren Betrieb des jeweiligen Zielobjekts beeinträchtigen? Durch vorhandene Zugangs- und Zugriffsberechtigungen sowie durch Insider-Wissen droht hier oft besondere Gefahr.
- Drohen besondere Gefahren durch Objekte, die nicht dem betrachteten Informationsverbund zuzurechnen sind? Solche *externen Objekte* können beispielsweise fremde Anwendungen, IT-Systeme oder bauliche Gegebenheiten sein. Die Definition des betrachteten Informationsverbunds dient dazu, den Untersuchungsgegenstand für die Sicherheitskonzeption festzulegen. Dies darf jedoch nicht dazu führen, dass Gefahren, die von außerhalb des betrachteten Informationsverbunds ausgehen, bei der Risikoanalyse vernachlässigt werden. Quellen für diese speziellen Gefährdungen sind beispielsweise
  - die Dokumentation des Herstellers,
  - Warn- und Informationsdienste von Computer Emergency Response Teams (CERTs), wie dem des BSI unter https://www.cert-bund.de,
- Publikationen über Schwachstellen im Internet (z. B. Threat Intelligence, Feeds) und eigene Bedrohungsanalysen.

9.4 Zusammenspiel mit ISO/IEC 31000

In den internationalen Normen zum Risikomanagement und zur Risikobeurteilung, insbesondere der ISO/IEC 31000, werden einige Begriffe anders belegt als es im deutschen Sprachraum üblich ist. In der folgenden Tabelle sind die wesentlichen Begriffe aus ISO/IEC 31000 und dem BSI-Standard 200-3 gegenübergestellt. Diese Gegenüberstellung dient der Zuordnung der Begriffe der ISO 31000 zu den Begriffen der BSI-Standards 200-2 und 200-3 (siehe Abbildung 7).

ISO/IEC 31000 und IT-Grundschutz

ISO/IEC 31000:2009	IT-Grundschutz
Establishing the context, Kapitel 5.3	**BSI-Standard 200-1** (siehe [BSI1]), Managementprinzipien, Kapitel 4 Planung des Sicherheitsprozesses, Kapitel 7.1 **BSI-Standard 200-2** Initiierung des Sicherheitsprozesses, Kapitel 3
Risk assessment, Kapitel 5.4	**BSI-Standard 200-3** Risikobeurteilung, Kapitel 1
• Risk Identification • Risk Analysis • Risk Evaluation	• Erstellung einer Gefährdungsübersicht • Risikoeinschätzung • Risikobewertung
Risk Identification, Kapitel 5.4.2	**BSI-Standard 200-3** Erstellung einer Gefährdungsübersicht, Kapitel 4
Risk Analysis, Kapitel 5.4.3	**BSI-Standard 200-3** Risikoeinschätzung, Kapitel 5.1
Risk Evaluation, Kapitel 5.4.4	**BSI-Standard 200-3**, Risikobewertung, Kapitel 5.2
Risk Treatment, Kapitel 5.5	**BSI-Standard 200-3**, Risikobehandlung, Kapitel 6
Communication and Consultation, Kapitel 5.2	**BSI-Standard 200-1**, Kommunikation und Wissen, Kapitel 4.2 **BSI-Standard 200-2** Informationsfluss im Informationssicherheitsprozess, Kapitel 5.2
Monitoring and Review, Kapitel 5.6	**BSI-Standard 200-1** Aufrechterhaltung der Informationssicherheit, Kapitel 7.4 Kontinuierliche Verbesserung der Informationssicherheit, Kapitel 7.5 **BSI-Standard 200-2** Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit, Kapitel 10 **BSI-Standard 200-3** Risiken unter Beobachtung, Kapitel 6.2

Tabelle 11: Gegenüberstellung der Begriffe aus ISO/IEC 31000 und dem BSI-Standard 200-3

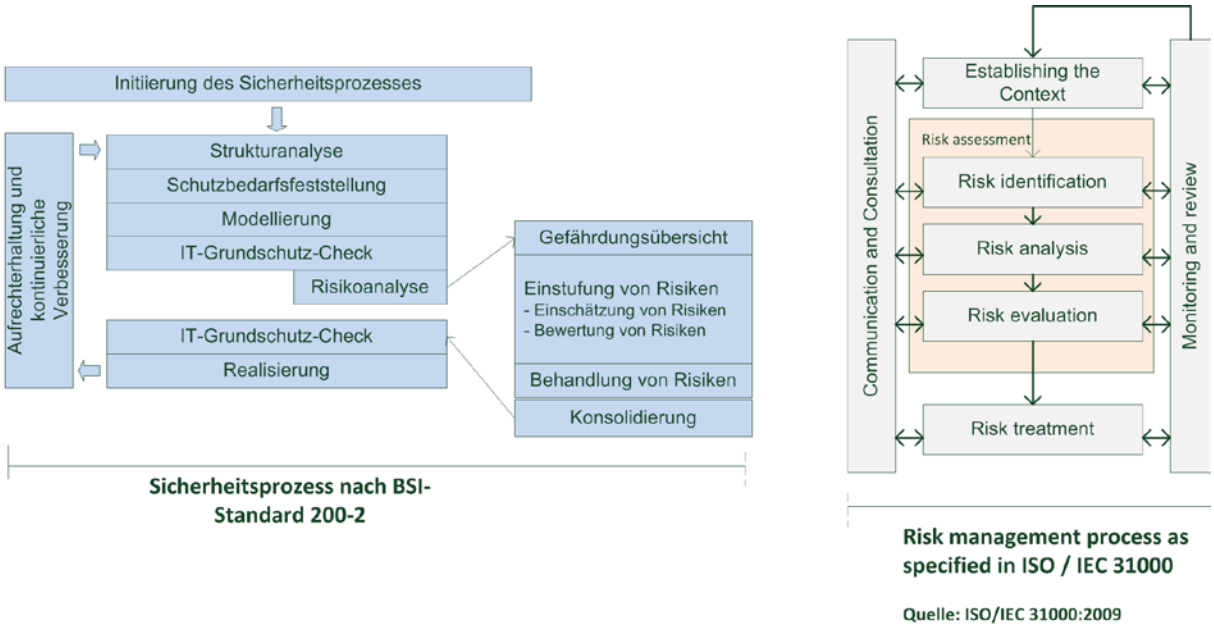


Abbildung 7: Sicherheitsprozess nach BSI-Standard 200-2 und Risikomanagementprozess nach ISO/IEC 31000

9.5 Literaturverzeichnis

[27005] ISO/IEC 27005:2011, International Organization for Standardization (Hrsg.), Information technology – Security techniques – Information security risk management, ISO/IEC JTC 1/SC 27, 2011

[31000] ISO/IEC 31000:2009, International Organization for Standardization (Hrsg.), Risk management – Principles and guidelines, ISO/TC 262, 2009

[31010] ISO 31000:2009, International Organization for Standardization (Hrsg.), Risk management – Risk assessment techniques, ISO/TC 262, 2009

[BSI1] Managementsysteme für Informationssicherheit (ISMS), BSI-Standard 200-1, Version 1.0, Oktober 2017, https://www.bsi.bund.de/grundschutz

[BSI2] IT-Grundschutz-Methodik, BSI-Standard 200-2, Version 1.0, Oktober 2017, https://www.bsi.bund.de/grundschutz

[BSI4] Notfallmanagement, BSI-Standard 100-4, Version 1.0, November 2008, https://www.bsi.bund.de/grundschutz

[GSK] IT-Grundschutz-Kompendium, BSI, jährlich neu, https://www.bsi.bund.de/grundschutz

[ISACA] Leitfaden ISO 31000 in der IT mit Vergleich zu anderen Standards, ISACA German Chapter e.V. und Risk Management Association e.V., Juni 2014, https://www.isaca.de/sites/pf7360fd2c1.dev.team-wd.de/files/attachements/2014_11_isaca-leitfadenanwendungderiso31000inderit.pdf

[Koenigs] IT-Risikomanagement mit System – Praxisorientiertes Management von Informationssicherheit und IT-Risiken, Hans-Peter Koenigs, Springer, 2013

[NIST800-30] Guide for Conducting Risk Assessments, NIST Special Publication 800-30, September 2012, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[SHB] IT-Sicherheitshandbuch – Handbuch für die sichere Anwendung der Informationstechnik, BSI, Version 1.0, März 1992, Bundesdruckerei