



IT-Sicherheitsmanagement





Inhaltsverzeichnis

Einleitung	15
1 Umfang und Aufgabe des IT-Security-Managements	21
1.1 Kapitelzusammenfassung	21
1.2 Einführung	21
1.3 Informationen und Daten	22
1.4 IT-Security-Management ist wichtig	24
1.5 Wie gefährdet sind die Unternehmensdaten	26
1.5.1 Sicht des Verfassungsschutzes	27
1.5.2 Öffentliche Wahrnehmung	27
1.5.3 Die eigene Wahrnehmung	29
1.6 Begrifflichkeiten	30
1.7 Selbstverständnis der IT-Security-Organisation	32
1.8 Grundregeln	35
1.9 Umfang des IT-Security-Managements	38
1.9.1 Pfeiler der IT-Security	39
1.9.2 Aufgaben des IT-Security-Managements	44
1.10 IT-Security zwischen Nutzen und Kosten	47
2 Organisation der IT-Security	49
2.1 Kapitelzusammenfassung	49
2.2 Einführung	49
2.3 Rollen innerhalb des IT-Security-Managements	50
2.3.1 Manager IT-Security	50
2.3.2 Unternehmensleitung	56
2.3.3 Weitere Rollen	56



INHALTSVERZEICHNIS

2.4	Verankerung im Unternehmen	58
2.4.1	IT-Security im Organigramm	58
2.4.2	IT-Security und der Datenschutz	65
2.4.3	Zusammenspiel mit anderen Sicherheitsbereichen	66
3	IT-Compliance	71
3.1	Kapitelzusammenfassung	71
3.2	Einführung	73
3.3	Standards	78
3.3.1	ISO-2700x-Reihe	79
3.3.2	Standards des Bundesamts für Sicherheit in der Informationstechnik	85
3.3.3	Gegenüberstellung ISO 2700x und BSI-Grundschutz	89
3.3.4	ITIL	92
3.3.5	Weitere Standards	93
3.4	Gesetze	94
3.4.1	EU-Datenschutz-Grundverordnung	95
3.4.2	IT-Sicherheitsgesetz	99
3.4.3	Weitere Gesetze	99
3.4.4	Branchenstandards am Beispiel TISAX	101
3.4.5	ISO 27001 und TISAX	104
3.4.6	Vorbereitende Maßnahmen	106
3.4.7	Fragekatalog	109
4	Organisation von Richtlinien	127
4.1	Kapitelzusammenfassung	127
4.2	Einführung	128
4.3	Strukturierung von Richtlinien	129
4.4	Beschreibung und Kategorisierung	130
4.5	Pflege und Lenkung von Richtlinien	131
4.6	Richtlinien und Audits	133



INHALTSVERZEICHNIS

4.7	Verschiedene Richtlinien	135
4.7.1	Sicherheitsrichtlinie	136
4.7.2	Klassifizierungsrichtlinie	141
4.7.3	ISMS-Handbuch	144
4.7.4	Richtlinie zum IT-Risikomanagement	146
4.7.5	IT-Sicherheitsrichtlinie	148
4.7.6	IT-Systemrichtlinien	152
4.8	Von der Theorie in die Praxis	153
5	Betrieb der IT-Security	155
5.1	Kapitelzusammenfassung	155
5.2	Einführung	155
5.3	IT-Security und der IT-Betrieb	157
5.4	Betriebliche Grundsätze	158
5.4.1	Ableitung aus gesetzlichen Vorschriften	158
5.4.2	Vertragswesen	159
5.4.3	Administrative Tätigkeiten	159
5.4.4	Trennung von Funktionen	160
5.4.5	Prinzip der geringsten Rechte	161
5.5	IT-Security-Prozesse	162
5.5.1	Zugangs- und Zugriffskontrolle	162
5.5.2	Sicherheit von Software	169
5.5.3	Sichere Softwareentwicklung	174
5.5.4	Identitätsmanagement	176
5.5.5	Genehmigungsprozesse	181
5.5.6	Standardisierung	182
5.5.7	Unterstützung des IT-Betriebs	183
6	IT Business Continuity Management	185
6.1	Kapitelzusammenfassung	185
6.2	Einführung	186
6.3	Abgrenzung der Begriffe	190



INHALTSVERZEICHNIS

6.4	IT-Notfallmanagement und Verfügbarkeitsmanagement	192
6.5	Gesetzliche Rahmenbedingungen des IT Business Continuity Managements	193
6.6	Business-Impact-Analyse	193
6.6.1	Erfassung und Priorisierung der Geschäftsprozesse	194
6.6.2	Business-Impact-Analyse in der Praxis	200
6.7	Weitere Einflussfaktoren	201
7	IT-Notfallmanagement	203
7.1	Kapitelzusammenfassung	203
7.2	Einführung	203
7.3	IT-Notfallmanagement	204
7.4	Richtlinie zum IT-Notfallmanagement	205
7.5	Ableitung von Notfallstrategien	206
7.6	IT-Notfallkonzepte erstellen	207
7.6.1	Schweregrade	209
7.6.2	Notfallvorsorge	211
7.7	Notfallorganisation	217
7.7.1	Organisationsstruktur	217
7.7.2	Kompetenzen und Zuständigkeiten	218
7.7.3	Notfallhandbuch	219
7.8	Notfallbewältigung	221
7.9	Notfallübungen	225
7.10	Überprüfung des IT-Notfallmanagements	226
7.11	Monitoring im Rahmen des IT Business Continuity Managements	227
7.12	Checklisten IT-Notfallmanagement	228
7.12.1	Checkliste Business-Impact-Analyse	228
7.12.2	Checkliste Notfallorganisation	229
7.12.3	Checkliste Notfallpläne und Wiederanlaufpläne	230
7.12.4	Checkliste Rechenzentrum	230



INHALTSVERZEICHNIS

8	Verfügbarkeitsmanagement	233
8.1	Kapitelzusammenfassung	233
8.2	Einführung	233
8.3	Richtlinie zum Verfügbarkeitsmanagement	234
8.4	Verfügbarkeit	235
8.4.1	Klassifizierung von Verfügbarkeit	236
8.4.2	Vorgehensweise	238
8.4.3	Berechnung der Verfügbarkeit	239
8.5	Ausfallsicherheit	240
8.6	Ausprägungen von Redundanz	241
8.6.1	Strukturelle Redundanz	242
8.6.2	Funktionelle Redundanz oder unterstützende Redundanz	243
8.6.3	Informationsredundanz	243
8.7	Redundante Hard- und Software	243
8.8	Virtualisierung	245
8.9	Bauliche Maßnahmen zur Steigerung der Verfügbarkeit	246
9	Technische IT-Security	249
9.1	Kapitelzusammenfassung	249
9.2	Einführung	250
9.3	Technisch-Organisatorische Maßnahmen	252
9.3.1	Zugangskontrolle	254
9.3.2	Zugriffskontrolle	259
9.3.3	Übertragungskontrolle und Transportkontrolle	261
9.3.4	Eingabekontrolle	265
9.3.5	Verfügbarkeitskontrolle, Wiederherstellbarkeit und Zuverlässigkeit	266
9.3.6	Datenintegrität	267
9.4	Verschlüsselung	268
9.4.1	Begriffsbestimmungen	269
9.4.2	Symmetrische Verschlüsselungssysteme	270
9.4.3	Asymmetrische Verschlüsselungsverfahren	271



INHALTSVERZEICHNIS

9.5	Cloud Computing	272
9.5.1	Dienstleistungen in der Cloud	276
9.5.2	Risikofaktoren	278
9.5.3	Datenschutzrechtliche Aspekte	285
9.5.4	Vertragliche Vereinbarungen	287
9.5.5	Sinnvolle Freigabeprozesse	288
9.6	Betrieb von Firewalls	290
9.6.1	Paketfilter und Application-Gateways	292
9.6.2	Firewall-Regelwerk	295
9.6.3	Internet-Proxyserver	297
9.7	Internetzugang und Nutzung von E-Mail	298
9.7.1	Risikofaktor E-Mail	299
9.7.2	Verschlüsselung von E-Mails	300
9.7.3	Risikofaktor Internetbrowser	301
9.8	Penetrationstests	302
9.9	Digitale Signatur	304
9.10	Intrusion-Detection-Systeme	306
9.11	Wireless LAN	308
10	IT-Risikomanagement	311
10.1	Kapitelzusammenfassung	311
10.2	Einführung	312
10.3	IT-Risikomanagement im Unternehmenskontext	312
10.4	Akzeptanz des IT-Risikomanagements	314
10.5	Operatives IT-Risikomanagement	315
10.5.1	Vorgehensweise	318
10.5.2	IT-Risikomanagementprozess	320
10.5.3	Übergeordnete Risikobetrachtung	322
10.5.4	Schwachstellen	325
10.5.5	Bedrohungen	328
10.5.6	Zusammenspiel von Bedrohungen, Schwachstellen und Maßnahmen	330
10.5.7	Verhältnismäßigkeit	332



INHALTSVERZEICHNIS

10.6	Schutzbedarfsfeststellung	333
10.6.1	Schutzziele	333
10.6.2	Schutzstufen	336
10.6.3	Prinzipien	337
10.6.4	Feststellung des Schutzbedarfs	338
10.6.5	Veränderung des Schutzbedarfs	343
10.6.6	Widersprüchliche Schutzziele	344
10.6.7	Schadensklassen	344
10.6.8	Abbildung des Datenflusses	345
10.6.9	Entscheidungsfindung auf Basis des Schutzbedarfs	346
10.7	IT-Risikomanagement Prozess	348
10.7.1	Risiken identifizieren	348
10.7.2	Risikoermittlung	353
10.7.3	Risikobewertung	356
10.8	Quantitative Darstellung von Risiken	359
10.8.1	Grundlagen der Risikoberechnung	360
10.8.2	Risikoberechnung im Beispiel	362
10.8.3	Risikomatrix	364
10.8.4	Risikokatalog	366
10.9	Risikobehandlung	368
10.9.1	Risiko akzeptieren	370
10.9.2	Risiko reduzieren	371
10.9.3	Risiko vermeiden	372
10.9.4	Risiko auf Dritte verlagern	372
10.10	Maßnahmen definieren	373
10.10.1	Maßnahmentypen	374
10.10.2	Individuelle Maßnahmenkataloge	375
11	Sicherheitsmonitoring	377
11.1	Kapitelzusammenfassung	377
11.2	Einführung	378
11.3	Ebenen des Monitorings	380



INHALTSVERZEICHNIS

11.4	System-Monitoring	382
11.4.1	Sicherheitsaspekte	383
11.4.2	Auswahl zu überwachender Systeme	383
11.4.3	Implementierung im Netzwerk	384
11.5	Protokoll-Monitoring	385
11.5.1	Unterstützung von Audits	386
11.5.2	Überwachung administrativer Tätigkeiten	387
11.5.3	Schwachstellenmanagement	388
12	IT-Security-Audit	391
12.1	Kapitelzusammenfassung	391
12.2	Einführung	392
12.3	Audits im Kontext des IT-Security-Managements	392
12.4	Audits im Unternehmenskontext	396
12.5	Audits nach Kategorien	397
12.6	Vor-Ort kontra Selbstauskunft	399
12.7	Anforderungen an den Auditor	400
12.8	Ein Audit Schritt für Schritt	402
12.8.1	Vorbereitung	403
12.8.2	Durchführung	404
12.8.3	Nachbereitung	408
12.8.4	Abschlussbericht	408
13	Management von Sicherheitsereignissen und IT-Forensik	413
13.1	Kapitelzusammenfassung	413
13.2	Einführung	414
13.3	Angriffe auf Ihre Daten	415
13.3.1	Durch eigene Mitarbeiter	416
13.3.2	Durch Außenstehende	418
13.3.3	Angriffe und Angriffsvektoren	418
13.3.4	Angriffsarten	419
13.4	Management von Sicherheitsereignissen	424



INHALTSVERZEICHNIS

13.5	IT-Forensik	426
13.5.1	Arten der IT-Forensik-Analyse	431
13.5.2	Einrichtung von Honeypots	432
13.6	Elemente der forensischen Untersuchung	433
13.6.1	Zielsetzung	434
13.6.2	Anforderungen an die Analyse	435
13.6.3	Forensische Methoden	436
13.6.4	Forensische Untersuchung	437
14	Kennzahlen	443
14.1	Kapitelzusammenfassung	443
14.2	Einführung	444
14.3	Die Aufgabe von Kennzahlen	444
14.4	Quantifizierbare Kennzahlen	447
14.5	Steuerung mithilfe von Kennzahlen	449
14.6	Qualität von Kennzahlen	451
14.6.1	Gute Kennzahlen	451
14.6.2	Schlechte Kennzahlen	452
14.6.3	Vergleichbarkeit von Kennzahlen	452
14.7	Verschiedene Kennzahlen aus der IT-Security	453
14.8	Kennzahlen im laufenden Verbesserungsprozess	458
14.9	Laufende Auswertung von Kennzahlen	460
14.10	Annualized Loss Expectancy	460
14.11	IT-Security Balanced Scorecard	463
14.11.1	Einführung der IT-Security Balanced Scorecard	465
14.11.2	Maßnahmenziele für den Bereich IT-Security	469
15	Praxis: Aufbau eines ISMS	473
15.1	Kapitelzusammenfassung	473
15.2	Einführung	474
15.3	ISMS in Kürze	474



INHALTSVERZEICHNIS

15.4	Herangehensweise	477
15.5	Schritt für Schritt zum ISMS	478
15.5.1	Plan-Do-Check-Act	482
15.5.2	Vorarbeiten	483
15.5.3	Plan: Gestaltung des ISMS	488
15.5.4	Do: Umsetzung der Arbeitspakete	503
15.5.5	Check: Überprüfung des ISMS	505
15.5.6	Act: Umsetzung von erkannten Defiziten	506
15.5.7	Dokumentation	506
15.6	Softwaregestützter Aufbau eines ISMS	511
15.6.1	Auswahl einer ISMS-Lösung	512
15.6.2	Darstellung der Risiken und der Unternehmenswerte	514
15.6.3	Darstellung von Prozessen	517
15.6.4	IT-Risikomanagement	518
15.6.5	Richtlinienmanagement	520
15.6.6	Arbeitsabläufe abbilden	521
15.6.7	Berichte erstellen	522
15.7	Zertifizierung nach ISO 27001	523
15.7.1	Ansprechpartner	525
15.7.2	Prinzipien	526
16	Awareness und Schulung	529
16.1	Kapitelzusammenfassung	529
16.2	Verbesserungsprozess	530
16.3	Voraussetzungen für eine Sicherheitskultur	531
16.4	Erfassung der Sicherheitskultur	533
16.5	Top-down-Ansatz	534
16.6	Awareness-Projekte	535
	Index	539



Einleitung

Anmerkung zur dritten Auflage

Die grundlegenden Bestandteile eines IT-Sicherheitsmanagements ändern sich nicht in ähnlich kurzen Zeiträumen, wie sich die technische Seite der IT und der IT-Security ändert. Die Schwerpunkte, die fachliche Ausgestaltung und die Prozesse bleiben davon aber nicht unbeeindruckt. Werden Daten vermehrt in Public Clouds verarbeitet, auf Mobiltelefonen gespeichert, über Chat-Apps geteilt oder im Rahmen von Industrie 4.0 in einer Größenordnung erhoben, die bislang kaum denkbar war, dann müssen sich die entsprechenden Maßnahmen der IT-Security an diese Veränderungen anpassen. Der Gesetzgeber hat parallel dazu die Aufgabe, Regelungen zu erlassen, um frühzeitig die Rahmenbedingungen festzulegen und dabei zu helfen, dem Missbrauch entgegenzuwirken. In diesem Zusammenhang werden weltweit neue Gesetze erlassen und entsprechende Kontrollgremien eingesetzt. Völlig unterschiedlich gelagerte Beispiele dafür sind die EU-Datenschutz-Grundverordnung (EU-DSGVO), das IT-Sicherheitsgesetz oder das China Cybersecurity Law. Alle diese Regelungen haben immense Auswirkungen darauf, wie Unternehmen Daten erfassen, verarbeiten, speichern oder austauschen dürfen. In der Fülle und der Bandbreite der neuen Regelungen liegt aber immer auch die immanente Gefahr, etwas falsch zu machen, weil man eben den falschen Weg gewählt hat, mit diesen Anforderungen umzugehen. Der Weg aus dieser Problematik ist es, einem Lösungsansatz zu folgen, der zum einen international bekannt und anerkannt ist und zum anderen auf einem stringenten Prozess-Modell basiert, das so angelegt ist, dass alle oben genannten Punkte abgedeckt werden können. Dieser Weg ist die Einführung eines IT-Sicherheitsmanagements auf Basis der ISO-27000-Normen-Familie unter Beachtung der datenschutzrechtlichen Bestimmungen der EU-DSGVO.

Auch wenn sich seit der 2. Auflage einiges auf dem Sektor der Informations sicherheit getan hat, so hat sich dennoch gezeigt, dass die Leitplanken, die durch die beherrschenden Normen der ISO-2700x-Reihe gelegt wurden, Bestand hatten und auch weiterhin Bestand haben werden. So richten sich an



EINLEITUNG

den Prozessmodellen dieser Normen in der Zwischenzeit nationale Gesetze genauso aus wie auch die Anforderungen von Unternehmen und dem öffentlichen Sektor. Diese Standardisierung und das damit einhergehende Ziehen am gleichen Seil ist auch bitter nötig. Die Zahl der täglich gemessenen gezielten Cyber-Angriffe steigt unaufhörlich weiter, während parallel deren Qualität im Durchschnitt immer weiter zunimmt.

Mit der Covid-19-Krise ändern sich die Angriffsvektoren und passen sich neuen Arbeitsprozessen an. Insbesondere Unternehmen, die kein umfassendes Sicherheitskonzept etabliert haben, bekommen dies zu spüren. Mitarbeiter arbeiten im weitgehend ungesicherten häuslichen Umfeld, Budgets werden eingefroren und personell ausgedünnte IT-Abteilungen werden der Masse an Makro- und Ransomware-Angriffen nicht mehr Herr. Jede Fehlkonfiguration an einem Server oder einer Sicherheitssoftware kann in einem solchen Umfeld schnell den Cyber-Supergau bedeuten. Für Unternehmen, die gleichzeitig in einem angespannten wirtschaftlichen Umfeld agieren, kann dies schnell auch das Aus bedeuten.

Niemals zuvor ist die Verflechtung von Lieferketten so offensichtlich zutage getreten wie nach den Lockdowns verschiedener Länder oder Regionen. Dies gilt auch für Datenflüsse zwischen Lieferanten und Herstellern und damit verwundert es nicht, dass die großen Branchenverbände längst damit begonnen haben, nicht nur diejenigen Daten sicher zu verarbeiten, die sie im eigenen Zugriff haben, sondern auch Lieferanten anzuhalten, Sicherheitsstandards einzuhalten. Aus diesem Grund habe ich ein Kapitel zu dem viel beachteten Branchenstandard der deutschen Automobilindustrie, der unter der Abkürzung »TISAX« bekannt ist, im Kapitel »Compliance« hinzugefügt. Sehr ähnliche Standards entstehen in vielen Branchen und letzten Endes werden sie sich aufgrund der gleichen Wurzeln auch nicht wesentlich voneinander unterscheiden.

Neben dem eben erwähnten neu hinzugefügten Sicherheitsfeld wurden in der vorliegenden Auflage viele Kapitel aktualisiert.

Ich möchte all denjenigen danken, die mir Input bezüglich neuer Gesichtspunkte gegeben haben. Dies schließt sowohl die wohlmeinende Kritik an einzelnen Punkten durch Leser als auch das Feedback meiner Studierenden und der Professoren an der Hochschule oder von Kollegen im Unternehmen mit ein. Auch wenn man sich selbst als Generalisten im IT-Sicherheitsbereich



sieht, ist man nicht ganz vom Tunneldenken befreit und übersieht doch das eine oder andere Mal neue Aspekte und neue Denkansätze – obwohl sie doch so offensichtlich vor einem liegen.

Über die Zielgruppe

Nicht alle Wege, aber zumindest sehr viele, führen nach Rom, und wohl ebenso viele Wege führen zum Job des IT-Security-Managers. Einige Kandidaten haben schon ein paar Jahre Berufserfahrung in ähnlichen Bereichen gesammelt, haben bereits einschlägige Erfahrungen gemacht oder kommen direkt aus dem Studium, in dem sie das Thema, zumindest theoretisch, schon behandelt haben.

Andere, und damit sind wir wieder bei den vielen Wegen angekommen, die zum Ziel führen, sind Neueinsteiger oder Quereinsteiger. Vielleicht kommen sie aus der IT-Abteilung und haben zuvor Server administriert oder Softwareprojekte geleitet. In manchen Fällen waren sie davor aber auch im Controlling oder in der Unternehmensplanung tätig und haben sich mit Qualitätsaudits oder Risikomanagement beschäftigt. Diese Kollegen stehen dann häufig vor der Herausforderung, dass sie, selbst wenn sie angekommen sind (nicht in Rom selbstverständlich, sondern am Arbeitsplatz des IT-Security-Managers), die schiere Menge an Einzelthemen dann fast erschlägt.

Beiden Gruppen kann man aufrichtig versichern, dass es kaum eine Aufgabe gibt, die vielschichtiger und vielseitiger gestaltbar ist, als diese. Gerade der Umfang schafft die Chance, dem Arbeitsplatz den eigenen Stempel aufzudrücken, und wenn man die Grundlagen einmal verstanden hat, fällt es schwer, sich eine spannendere Aufgabe vorzustellen. Das Gebiet der IT-Security ist nicht so alt, als dass es bereits fest ausgetretene Pfade gäbe. Vielmehr gehen die Meinungen, was denn ein IT-Security-Manager zu tun hat, weit auseinander. Damit muss sich die IT-Security-Organisation dem Unternehmen flexibel anpassen. Stetige Veränderungen, hinzukommende Verknüpfungen mit anderen Abteilungen und die laufende Kommunikation mit denen, die Daten verarbeiten, und denen, die sie verwalten, bringen einerseits Abwechslung und andererseits den Druck, laufend hinzuzulernen.

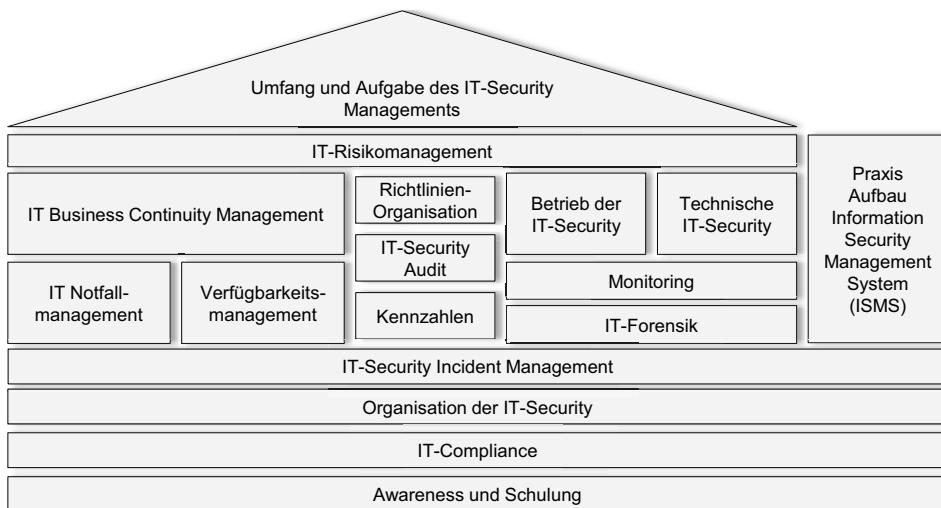
Für alle, die frisch einsteigen, schon Erfahrungen haben oder gar aus einem ganz anderen Fachgebiet heraus quereinsteigen und nun auf einfache, aber



EINLEITUNG

doch umfassende Art in die Thematik IT-Security eingeführt werden wollen, ist das vorliegende Buch gedacht.

Aufbau des Buches



Für eine strukturierte Vorgehensweise beim Durcharbeiten des Buches ist es sinnvoll, mit dem ersten Kapitel »Umfang und Aufgabe des IT-Security-Managements« zu beginnen. Im Grunde umreißt es das Aufgabengebiet und bringt die verschiedenen Themen in einen Zusammenhang. Ein guter Einstieg, um danach zielgerichtet diejenigen Kapitel zu betrachten, die einem selbst am interessantesten erscheinen. Aus diesem Grund sind alle Kapitel so verfasst, dass ein direkter Einstieg erleichtert wird.

Ansonsten gilt: Für ein durchgängiges Verständnis und als eine Art roter Faden ist es empfehlenswert, sich erst um Fundament und Dach zu kümmern, bevor die verschiedenen Säulen abgearbeitet werden.

Jedes Kapitel beschreibt einen zusammenhängenden Themenbereich der IT-Security. Der Aufbau bleibt dabei immer ähnlich. Obligatorische Theorie wechselt sich ab mit Tipps aus der Praxis für die Praxis, ein paar Beispielen und dazu Aufzählungen und Checklisten als Hilfestellung. Die einzelnen Themen umfassen dabei das notwendige Wissen, um den Arbeitsplatz IT-Security ausfüllen zu können, und häufig noch etwas mehr.



Die Aufgaben eines IT-Security-Managers sind vielfältig und abwechslungsreich, bauen aber immer wieder aufeinander auf. Es gibt Themen wie das IT-Risikomanagement, die in den verschiedensten Fragestellungen immer wieder auftauchen. So ist das Wissen notwendig, wie eine Risikobewertung durchgeführt wird, wenn es darum geht, Prioritäten in der Notfallvorsorge zu treffen, aber genauso auch im alltäglichen Betrieb, wenn es um die Berechtigungsvergabe oder die Entscheidung für und wider einer einzukaufenden Software geht. Aus diesem Grund wird dieses Aufgabenfeld als Teil der Dachkonstruktion in der Abbildung abgebildet.

Die weiteren Elemente des Hauses stellen die anderen Kapitel des Buches dar. Manche Themen bilden das Fundament für den gesamten Komplex, wieder andere bilden zusammen mit einem oder zwei Bereichen eine Einheit. So sind die Kapitel zum IT-Notfallmanagement und zum Verfügbarkeitsmanagement zwei Teile des übergeordneten Themas IT Business Continuity Management.

Die Wahl, die IT-Security-Organisation, die IT-Compliance, das IT-Security Incident Management und die Bildung von Awareness als Fundament zu nutzen, fiel aufgrund der Tatsache, dass es nicht möglich ist, sie immer und immer wieder mitzubetrachten. Gleichgültig, welche Maßnahme implementiert oder welche Richtlinie durchgesetzt werden soll, immer stellt sich die Frage, wie diese zu kommunizieren und zu schulen ist, wie die inneren und äußeren Anforderungen aussehen und wie die IT-Security-Organisation aufgebaut sein muss, um dies auch bewältigen zu können.

Ein Kapitel sticht etwas hervor. Das reine Praxiskapitel über die Einführung eines Information Security Management Systems (ISMS) steht etwas abseits am rechten Rand des Hauses. Diese Zuordnung soll vergeben, dass alle im Buch behandelten Themen in irgendeiner Art und Weise Teil des ISMS sind. Die Zusammenführung und die Annäherung an die Praxis werden an dieser Stelle vertieft angegangen.



1 Umfang und Aufgabe des IT-Security-Managements

1.1 Kapitelzusammenfassung

Im Rahmen des ersten Kapitels werden die einzelnen Themengebiete des IT-Security-Managements in einen Gesamtzusammenhang eingebettet. Es wird erläutert, warum man Informationen schützen muss und wie diese Aufgabe durch die IT-Security-Organisation wahrgenommen wird.

Die Top-5-Fragen zum aktuellen Kapitel:

- Sind die Aufgabengebiete definiert, die dem IT-Security-Management zugeordnet werden?
- Sind die organisatorischen Einheiten, die sich um die Betreuung von sicherheitsrelevanten Systemen kümmern, darüber informiert und dahin gehend instruiert, dass sie sich im Einflussbereich des IT-Security-Managements befinden?
- Wurden Schutzziele zusammen mit der Unternehmensleitung definiert?
- Werden die Grundregeln (Prinzipien) im Umgang mit Informationen kommuniziert und in der Praxis umgesetzt?
- Werden die Grundpfeiler der IT-Security, das IT-Risikomanagement, die IT-Compliance und die IT-Governance auch in Verbindung mit dem IT-Security-Management gebracht und damit auch als Aufgabe des Managers IT-Security gesehen?

1.2 Einführung

Ransomware, Industrie 4.0, die EU-Datenschutz-Grundverordnung, Mobility, Heimarbeitsplätze, Public-Cloud-Services und viele andere Themen haben in letzter Zeit die Schlagzeilen beherrscht. Angesichts der Wucht dieser Themen und den häufig noch fehlenden, umfassenden Sicherheitsarchitekturen, die man benötigt, um diese zu beherrschen, geht immer häufiger das Gefühl

**KAPITEL 1 – UMFANG UND AUFGABE DES IT-SECURITY-MANAGEMENTS**

dafür verloren, wie diese Sicherheits-Felder miteinander verwoben sind, und vor allem auch, wie diese mit den klassischen Sicherheitsanforderungen wie dem Assetmanagement oder auch einem Antivirenkonzept verknüpft werden müssen. Altes Wissen trifft dabei auf völlig neue Bedrohungen. In dieser Gemengelage ist es die Aufgabe des Managers IT-Security, den Überblick zu bewahren und auf die wichtigen Bedrohungen mit den erforderlichen Maßnahmen in angemessener Weise zu reagieren. Im Sprachgebrauch dieses Buches unterscheidet er sich damit von einem IT-Security-Experten, der Fachmann für ein dediziertes Feld der IT-Security ist und sich vorwiegend auch nur innerhalb dieses Arbeitsgebiets bewegt.

Der Manager IT-Security sieht sich in der Situation, das Know-how des Unternehmens zu schützen, indem er Bedrohungen erkennt, abschätzt und diesen dann geeignete Sicherheitskonzepte und Maßnahmen entgegengesetzt. Zu diesem Zweck bedient er sich Werkzeugen, die in diesem Buch dargestellt werden. Diese Werkzeuge haben sich über die Jahre bewährt und in der Zwischenzeit auch international durchgesetzt. Aus diesem Grund ist es nicht überraschend, dass sich eine recht junge EU-Datenschutz-Grundverordnung der gleichen Prozesse bedient wie eine »ältere« ISO-27001-Norm.

1.3 Informationen und Daten

Der Schutz von Informationen, also dem Know-how des Unternehmens, ist die Aufgabe des IT-Security-Managements. Nur was sind Informationen und worin unterscheiden sie sich von Daten? Daten sind eine technische Darstellung von Informationen. Anders ausgedrückt: Informationen sind Daten, die einen Sinn ergeben. Auf niedrigster Ebene bestehen sie aus den physikalischen Zuständen »hohe Spannung« oder »niedrige Spannung« oder übersetzt null oder eins. Somit sind Daten zunächst einmal Bits und Bytes, deren Interpretation wiederum Informationen ergeben. Sicherheitsmaßnahmen wiederum kann man nicht direkt auf Informationen beziehen. Setzt man Verschlüsselung ein, dann werden die Daten verschlüsselt. Installiert man einen VirensScanner, dann schützt man das Betriebssystem und indirekt wieder die Daten. Ganz anders, wenn man dies aus der Perspektive des Risikomanagements betrachtet, dann stehen die Informationen im Mittelpunkt und deren Wert für das Unternehmen. Wenn wir also von Informationsschutz sprechen, dann geht es im Grunde darum, alle Systeme inklusive der Daten technisch zu



schützen, um die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen zu bewahren.

Die Gewinnung von Informationen aus einem Pool von Daten geschieht durch eine Fragestellung. So sind Daten mit der Ausprägung »4 Eier, 450 g Mehl, 400 ml Milch, Vanillezucker, 210 g Zucker und eine Prise Salz« nur im Zusammenhang mit der Frage »Was benötige ich, um vernünftige Pfannkuchen machen zu können?« als Information anzusehen. Ohne Fragestellung sind es nur beliebige, nicht zusammenhängende Daten. Daraus kann man ersehen, dass Daten zunächst einmal keinen Kontextbezug haben. Das wertvolle Gut, das es zu schützen gilt, ist also mehr als nur eine Menge von Bits und Bytes auf Festplatten.

Jede Form von Informationen, wie immer sie auch ausgestaltet sein mögen und deren Verlust einen Schaden für das Unternehmen bedeutete, gehört zu den Unternehmenswerten, die im Fokus des Managers IT-Security liegen.

1

Wichtig

Auch wenn sich das IT-Security-Management auf Daten und Daten verarbeitende Systeme konzentriert, stehen noch eine ganze Reihe weiterer Unternehmenswerte im Fokus der IT-Security. Dazu zählen auch abstrakte Werte wie der Ruf des Unternehmens oder das Wissen in den Köpfen der Mitarbeiter.

Informationen können in vielfältiger Form vorliegen. Die Erfahrungen von Mitarbeitern gehören genauso zu den schützenswerten Informationen wie Informationen, die auf Datenträgern vorliegen und durch IT-Systeme verarbeitet werden. Im Gegensatz zu Ersteren können Informationen, die auf Datenträgern wie Festplatten oder auf Papier vorliegen, generell geschützt werden. Deshalb konzentrieren sich viele Maßnahmen der IT-Security auf diese Art der Informationen.

Informationen haben einen Lebenszyklus und einen je nach Alter unterschiedlichen Schutzbedarf. So sind Informationen über eine technische Neuentwicklung zunächst einmal sehr sensibel, da der Schaden bei Verlust in diesem Stadium am höchsten wäre. Wird die Neuentwicklung zur Serienreife gebracht, so ist der Schutzbedarf vielleicht immer noch hoch, aber nicht mehr

23



KAPITEL 1 – UMFANG UND AUFGABE DES IT-SECURITY-MANAGEMENTS

so hoch wie zu Anfang. Dies ändert sich dann weiter, wenn die Produktion und Auslieferung beginnt. Ab diesem Zeitpunkt kann auch ein Konkurrent leicht auf das Produkt zugreifen und erforderliche Informationen extrahieren. Der Schutzbedarf ist in dieser Phase damit deutlich niedriger als zu Beginn.

Wichtig

Der Wert einer Information hängt von seiner generellen Bedeutung für das Unternehmen, seiner Qualität, seinem Alter und letztendlich von den Kosten ab, die bei ihrem Verlust oder der Nichtverfügbarkeit entstehen würden.

1

Informationen sind unterschiedlich wichtig, eine Tatsache, die sich in der Bewertung auf Basis der Klassifizierungsrichtlinie widerspiegeln muss. Diese dient dazu, Unternehmenswerte nach Schutzbedarf einzustufen. Im Rahmen der Verfügbarmachung von Informationen spielt es noch eine Rolle, inwieweit unwichtige Informationen herausgefiltert werden können. Dazu zählen Informationen, die für den Betrieb des Unternehmens keinerlei Rolle spielen und deren Vermischung mit relevanten Informationen Zeit und Ressourcen kosten. Zu diesen unwichtigen Informationen kann man z.B. Spam-E-Mails zählen.

Die Klassifizierung von Informationen ist ein wichtiges Instrument für den Manager IT-Security, weil sie aufzeigt, worauf er sich konzentrieren muss und worauf nicht. Außerdem bildet sie die Grundlage für das IT-Risikomanagement. Der Prozess der Einstufung von Unternehmenswerten wird unter aktiver Mithilfe des Erstellers der Information durchgeführt und hat weitreichende Auswirkung auf die Speicherung, die Verarbeitung, den Zugang und das Backup der Information.

1.4 IT-Security-Management ist wichtig

In Unternehmen, in denen ein organisatorischer Bereich IT-Dienstleistungen erbringt, ohne direkt Teil der Wertschöpfungskette zu sein, wird es schwerer fallen, IT-Security zu leben, als in einem Unternehmen, dessen Selbstzweck aus IT-Dienstleistungen besteht. Unternehmen, deren IT-Leistung in der Unternehmensspitze repräsentiert wird, haben wiederum einen administrativen Vorteil gegenüber Unternehmen, in denen dies nicht der Fall



ist. Diese Zusammenhänge lassen sich immer wieder finden und durchziehen alle Unternehmen. Damit im Zusammenhang steht die Tatsache, dass IT-Security immer noch stark als IT-Thema gesehen wird und häufig nicht die Unternehmensleitung, das Controlling oder der Vorstand als Treiber und Förderer in Erscheinung tritt. Diese Sichtweise ist einem laufenden Wandel unterzogen und es ist zu erkennen, dass sich dies in vielen Ländern immer schneller ändert. So hat das in Deutschland seit Juli 2015 gültige Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, das IT-Sicherheitsgesetz (IT-SiG), dazu geführt, dass Unternehmen, die kritische Infrastrukturen betreiben, mit hohem Aufwand Sicherheitsmanagementsysteme implementiert haben. Mit der Version 2.0 dieses Gesetzes wird der Geltungsbereich auf noch deutlich mehr Unternehmen ausgeweitet, was wiederum einen neuen Schub mit sich bringen wird. Auf europäischer Ebene sind weitere Richtlinien in der Ausarbeitung, die diesen Schwung noch verstärken werden.

1

In Ländern wie den USA hat man bereits früher damit begonnen. Der Grund hierfür liegt auch in der sich schnell weiterentwickelnden Gesetzgebung. So haben die Skandale um die Firmen Enron und WorldCom hohe Wellen geschlagen, die bereits 2002 im Sarbanes-Oxley Act mündeten. Dieses Gesetz soll die Verlässlichkeit von Finanzdaten amerikanischer Firmen sicherstellen, und dafür greift es tief in die Nachvollziehbarkeit administrativer Handlungen im Umgang mit Daten ein. Eine ganze Reihe an Prozessen und Vorgehensmodellen müssen umgesetzt werden, um dies zu erreichen, und die meisten davon zielen in die gleiche Richtung wie ein umfassendes IT-Security-Management.

Das führt zu dem zugegebenermaßen nicht repräsentativen Bild, dass ein Softwareunternehmen, das mit dem Verkauf von Applikationen seinen Umsatz erzielt, von vornherein eher darauf bedacht sein wird, dass die Innovationen, die im Produkt stecken, vertraulich bleiben, als ein Unternehmen der Chemiebranche mit mindestens ebenso sensiblen Daten. Das zeigt die Erfahrung der letzten Jahre und das viele Feedback auf entsprechende Umfragen.

Worin liegt aber nun der Unterschied zwischen Unternehmen A, das, sagen wir mal, Dünger verkauft, und Unternehmen B, das sein Geld mit innovativer Grafiksoftware verdient? Zum einen liegt es vermutlich daran, dass in Unternehmen B Menschen beschäftigt sind, die innerhalb des großen Feldes der IT arbeiten. Programmierer und Administratoren, die sich ständig austauschen und die schon von Berufs wegen eine starke Affinität zu dieser Thematik haben. In Unternehmen B arbeiten vor allem Ingenieure an den neuen Pro-



KAPITEL 1 – UMFANG UND AUFGABE DES IT-SECURITY-MANAGEMENTS

dukten. Sie tun dies zwar, indem sie Computer für die Modellierung benutzen, aber im Grunde ist die IT eine Abteilung, die nur dafür zu sorgen hat, dass diese Arbeit reibungslos vonstattengeht. Sie sollte sich also, möglichst unsichtbar, im Hintergrund halten.

Hebt man den Blick an und konzentriert sich auf die strategische Ebene, dann verschwinden die Unterschiede sehr schnell, und es wird ersichtlich, dass die Aufgabe des IT-Security-Managements aus genau den gleichen Gründen wichtig für beide Unternehmen ist.

Folgende Grundsätze sollen verdeutlichen, warum das IT-Security-Management eine unternehmerische Kernaufgabe darstellt – unabhängig von Geschäftszweck und auch unabhängig von der Unternehmensgröße:

1

- **IT-Security ist wichtig für alle Unternehmen**, die Know-how besitzen, das sie zu einem wichtigen Player auf dem Markt macht.
- **IT-Security ist wichtig für alle Unternehmen**, die Konkurrenten auf dem Markt haben.
- **IT-Security ist wichtig für alle Unternehmen**, die Technologien einsetzen, die verwundbar gegenüber Angriffen sein könnten.
- **IT-Security ist wichtig für alle Unternehmen**, die personenbezogene Daten speichern und verarbeiten.

Wenn man die Dinge von dieser Warte aus sieht, dann gibt es keine Unterschiede mehr zwischen Düngerherstellern, Softwareproduzenten oder öffentlichen Einrichtungen. Die Implementierung eines IT-Security-Managements ist für alle Unternehmen aller Geschäftsfelder entscheidend, um auf dem freien Markt bestehen zu können.

Die Unterschiede liegen dann nur noch in der Handhabung und Bewertung der verschiedenen Sicherheitsprozesse begründet. Also darin, wie man Risiken bewertet und davon abgeleitet, welches Budget man investiert, um Maßnahmen zur Risikoreduzierung zu installieren.

1.5 Wie gefährdet sind die Unternehmensdaten

Staatliche und private Stellen versuchen, die globale Gefährdungslage regelmäßig zu erfassen und geeignet darzustellen. Aus dieser Darstellung lassen sich Trends ableSEN, die der Unternehmensleitung ein unabhängiges Bild



WIE GEFÄHRDET SIND DIE UNTERNEHMENDATEN

ermöglichen, bevor sie daran geht, die dort gesammelten Informationen auf das eigene Unternehmen abzubilden.

1.5.1 Sicht des Verfassungsschutzes

Die Landesämter für Verfassungsschutz, die sich gezielt mit dem Thema Wirtschaftsspionage beschäftigen, touren seit einigen Jahren ohne Unterlass durch die Unternehmen und geben eine Einschätzung, was ihrer Erfahrung nach im Bereich des professionellen Datendiebstahls vor sich geht. Und die Zahlen, die sie dabei präsentieren, haben es in der Tat in sich. Es geht nicht nur um konkrete Beispiele, die bemüht werden, sondern darum, dass die Menge aufgedeckter staatlicher Spionageaktionen exponentiell steigt und dass sich ihrer Ansicht nach viele Staaten angesichts des weltweiten Konkurrenzkampfs im Wirtschaftssektor nicht mehr anders zu helfen wissen, als die Informationen zu stehlen, die sie benötigen. Im Gegensatz zu früher trifft es dabei nicht mehr nur die ganz großen Unternehmen, vielmehr rücken die Mittelständler in den Fokus. Unternehmen mit wenigen Tausend Mitarbeitern, die auf einem Sektor technologisch weit vorne mit dabei sind, werden zum Zielobjekt. Zur Zielerreichung wird laut Verfassungsschutz die ganze Bandbreite an Angriffsmöglichkeiten genutzt. Das reicht von Angriffen über das Internet über eigens für einen Angriff entwickelte Trojaner bis hin zum lokal durchgeführten Spionageangriff durch studentische Hilfskräfte oder Diplomanden.

Ein Zitat von der Webseite des baden-württembergischen Verfassungsschutzes drückt es so aus: »Der Verfassungsschutz sieht in den internetgebundenen Angriffen auf Netzwerke und Computersysteme von Firmen und Regierungsstellen die aktuell gefährlichste Bedrohung im Bereich Wirtschaftsspionage.« Hilfestellungen gibt das Amt auch: Es verweist auf die Schriften des Bundesamts für Sicherheit in der Informationstechnik (BSI), und dort wiederum wird das IT-Security-Management als der Prozess beschrieben, der eingeführt werden muss, um die Sicherheit des eigenen Know-hows und damit den Fortbestand des Unternehmens zu sichern.

1.5.2 Öffentliche Wahrnehmung

Wenn es erforderlich wird, zumeist abstrakte Gefährdungen mit Daten und Fakten zu hinterlegen, dann werden die eher generellen Verdachtsmomente und die wenigen konkreten Beispiele des Verfassungsschutzes im Zweifels-



KAPITEL 1 – UMFANG UND AUFGABE DES IT-SECURITY-MANAGEMENTS

fall nicht ausreichen, um die nötigen Mittel bewilligt zu bekommen, die erforderlich sind, ein modernes IT-Security-Management aufzubauen. Für diesen Zweck sind einige Quellen im Internet hilfreich, die sich seit Jahren bemühen, Vorfälle zu sammeln und statistisch darzustellen. Das Problem dabei ist grundsätzlich, dass niemand gerne darüber spricht, wenn er zum Mittelpunkt eines erfolgreichen Angriffs geworden ist. Angst um die eigene Reputation oder die Sorge, verklagt zu werden, falls auch anvertraute Daten gestohlen wurden, tun ihr Übriges.

Der Schaden einer Veröffentlichung wird somit häufig höher eingeschätzt als der Nutzen einer Anzeige. Das liegt auch daran, dass der Prozentteil an aufgeklärten Vorfällen verschwindend gering ist. Während große, publikums-wirksame Vorfälle auch von staatlichen Stellen verfolgt werden, bleibt es kleinen Unternehmen häufig selbst überlassen, Nachforschungen anzustellen. Auch heute noch sind die allermeisten Polizeidienststellen nicht in einem Maß ausgerüstet, das sie in die Lage versetzen würde, selbst erfolgreich tätig werden zu können.

Ein zweiter wichtiger Grund, warum viele Vorfälle niemals veröffentlicht werden, ist der, dass sie schlicht und einfach nicht entdeckt werden. Schätzungen gehen bis an die 90 % aller Vorfälle, die niemand bemerkt. Das hängt damit zusammen, dass Systeme zur Entdeckung von Sicherheitsvorfällen, sogenannte Intrusion-Detection-Systeme (IDS), nur in wenigen Unternehmen eingesetzt werden und aufgrund ihrer Komplexität selbst dort nur selten durchgängig brauchbare Ergebnisse liefern. Dazu kommt, dass ein solches System nur einen Baustein auf dem Weg zur Einführung eines IT-Security-Managementprozesses darstellt. Ohne entsprechende Prozesse, in die ein IDS eingebunden werden kann, ist die erfolgreiche Nutzung fast nicht möglich.

Aus nachvollziehbaren Gründen sind die Analysen der verschiedenen Institutionen nicht geeignet, wenn es darum geht, von den vorliegenden Aussagen konkrete Informationen abzuleiten, die auf das eigene Unternehmen eins zu eins abgebildet werden können. Das ist aber auch nicht immer erforderlich. Zumeist reichen die dort zusammengetragenen Informationen aus, um eine Entwicklung abzulesen und daraus eigene Schlüsse abzuleiten, was die Priorisierung von Themen angeht.

Aus Studien seit 2010/2011 ist der Verlauf sichtbar, den die Bedrohung Schadsoftware im Vergleich mit der Bedrohung Phishing seit 2005 nimmt. War 2005 das Auftreten von Schadsoftware das größte Problem, so hat sich dies



2007 umgedreht. Seit 2015 macht das Schreckgespenst »CEO Fraud« die Runde und mehrere namhafte Unternehmen wurden seitdem dazu gebracht, große Summen aufgrund gefälschter E-Mails an Diebe zu überweisen. Ab 2017 kam zu diesem Problem noch eine recht neue Disziplin hinzu, die sogenannte Erpressersoftware (*ransomware*), die einige technischen Schaden angerichtet hat. Gerade diese Art von Angriff bietet ein recht gutes Auskommen bei sehr geringem Risiko und deshalb finden Angriffe dieser Art auf zum Teil hochprofessionellem Wege statt. Alle Arten von Angriffen werden nun zunehmend professioneller ausgeführt und die Anzahl zielgerichteter und damit maßgeschneiderter Angriffe hat seit 2019 massiv zugenommen. Dementsprechend steigen auch die Schadenssummen an.

Was sich zeigt, ist, dass es nicht genügt, auf diesen Strauß an Angriffsarten mit Einzelmaßnahmen zu antworten. Das Bewusstsein für die aktuell größte Gefahr wird immer noch aus Studien, aus Berichten in Film, Funk und Fernsehen und der Werbung der Sicherheitsindustrie abgeleitet. Was man dabei schnell vergisst, ist: Studien werden über längere Zeiträume verfasst, und selbst wenn sich ein Trend herausbildet, wäre die Reaktionszeit zu hoch, um jedes Mal gezielt auf Verschiebungen der eingesetzten Angriffsmittel zu reagieren. Was aber in jedem Fall abgelesen werden kann, sind die Hauptangriffswege und damit die Hauptgefahren. Dementsprechend können auch die Prozesse der IT-Security ausgerichtet werden. Ableiten kann man daraus für jeden Verantwortlichen für IT-Security, dass nur ein umfassendes IT-Security-Management, das alle Bedrohungen und alle damit verbundenen Angriffsvektoren einkalkuliert, ein transparentes und verlässliches Sicherheitsniveau gewährleisten kann.

1.5.3 Die eigene Wahrnehmung

Wie sicher fühlt man sich im Unternehmen? Wie schätzt man die Bedrohungslage realistisch ein? Ist wirklich jemand oder etwas hinter dem Know-how des Unternehmens her und versucht, an dieses heranzukommen? Diese Fragen stellen sich zahllose Unternehmen und haben dabei eines gemeinsam: Objektive Antworten auf diese Fragen kann es nur in Einzelfällen geben, und deshalb beantworten Unternehmen diese Fragen aufgrund einer subjektiven Wahrnehmung. Damit wird auch gleich eine Antwort auf das Phänomen gegeben, warum jeder medial ausgeschlachtete, große Fall von Schadsoftware oder Datendiebstahl bei weithin bekannten Unternehmen branchenübergreifenden Aktionismus auslöst. Kurze Zeit später, die Medien sind bereits weiterge-



zogen, verlaufen viele dieser Aktionen im Sande, werden aus Kostengründen eingestellt oder nur unter Sparflamme weiterverfolgt.

Um ein annähernd genaues Bild von der Realität zu bekommen, ist es also erforderlich, möglichst viele Fakten zu kennen und zu bewerten. Die Analysen des Verfassungsschutzes, Statistiken von unabhängigen Gesellschaften kombiniert mit den Ergebnissen von Protokollen der eigenen Firewall und eigenen IDS-Systemen ergeben eine Momentaufnahme, die als Grundlage für die Sicherheitsstrategie dienen kann. Damit werden Informationen, die einen Durchschnitt abbilden, mit Informationen kombiniert, die tatsächliche, individuell aufgetretene Ereignisse beschreiben.

An diesem Punkt setzen Awareness-Maßnahmen an. In einem Top-down-Vorgehen werden die einzelnen Entscheidungsebenen laufend und möglichst mit faktenbasiertem Material über die Gefährdungslage informiert. Damit wird eine Grundlage geschaffen, vom reflexartigen Reagieren hin zum proaktiven Handeln zu gelangen. Den dann erreichten Zustand und die definierte weitere Vorgehensweise sowie die zugrunde liegenden Ziele kann man dann als IT-Security-Strategie umschreiben.

1.6 Begrifflichkeiten

Der Begriff »IT-Sicherheitsmanagement« beinhaltet bereits in seinem Namen eine Einschränkung: Es geht ganz offensichtlich um eine Aufgabe innerhalb der IT, besser ausgedrückt, um eine Aufgabe innerhalb der Abteilung, die sich mit der Informationstechnologie beschäftigt. Wenn man nun aber den Prozess der Wertschöpfung eines Unternehmens betrachtet, dann fällt schnell auf, dass sich, um ein Produkt herzustellen, viele zu schützende Unternehmenswerte überhaupt nicht im Einflussgebiet der IT bewegen. Dazu kann der Prototyp gehören, dessen Form von Hand hergestellt wird, oder die Kalkulation, die von einem Controller auf ein Flipchart aufgeschrieben und im Besprechungszimmer vergessen wird. Wenn man die Schutzmaßnahmen betrachtet, die erforderlich sind, um Informationen oder auch den Prototyp von eben zu schützen, dann wird dies noch deutlicher. Die ISO 27002 führt diesbezüglich eine ganze Reihe an Maßnahmen auf, wie den Gebäudeschutz inklusive des Zauns um den Entwicklungsstandort. So gesehen deckt die IT-Security einen großen Teil der in den einschlägigen Standards beschriebenen Themenfelder ab, aber eben nicht alle. Folgt man dieser Logik, dann kann die



IT-Security als Untermenge der Informationssicherheit gesehen werden. Die Informationssicherheit wiederum kann um sicherheitsrelevante Themen wie den Reiseschutz oder den Werkschutz ergänzt werden. Was letztendlich welchem Oberbegriff zugeschlagen wird, ist individuell in jedem Unternehmen zu regeln. Wichtig ist nur, dass die Trennung klar kommuniziert ist, um Reibungspunkte zu vermeiden. Aus diesem Grund werden diese Aufgaben in großen Unternehmen meistens gebündelt und einem Gesamtverantwortlichen unterstellt. Seitdem die EU-Datenschutz-Grundverordnung im Mai 2018 in Kraft getreten ist, steht an der Spitze einer solchen Organisation immer häufiger der Datenschutzbeauftragte.

Im Rahmen dieses Buches sprechen wir durchgehend von der IT-Security, dem Manager IT-Security und dem IT-Security-Management, weil es sich vorwiegend auf die Aufgaben innerhalb der Informationstechnologie bezieht. Wenn angrenzende oder nicht klar abgegrenzte Themengebiete angesprochen werden, z.B. wenn der Schutz von Rechenzentren zur Sprache kommt, die man gut und gerne dem physischen Schutz und damit z.B. dem Facility-Manager zuordnen kann, dann wird auf diesen Sachverhalt hingewiesen.

In der Diskussion rund um den Themenbereich »IT-Security« taucht eine Reihe von weiteren Begriffen auf, die zum Teil synonym verwendet werden. Dazu gehören zum einen der Begriff »Datenschutz« und zum anderen die Begriffe »Informationsschutz«, »Informationssicherheit«, »Datensicherheit«, »Cyber Security« oder »IT-Sicherheit«. Der Datenschutz, auf Englisch »data privacy«, bezieht sich dabei auf personenbezogene Informationen, deren Speicherung und Verarbeitung in der EU-Datenschutz-Grundverordnung und den länderspezifischen Gesetzen geregelt werden.

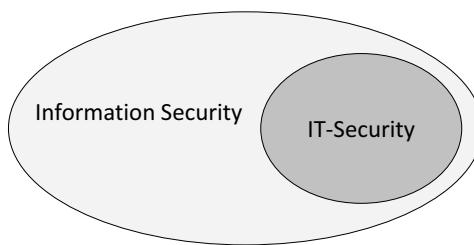


Abbildung 1.1: Schnittmenge Information-Security und IT-Security

Die Begriffe »Informationsschutz«, »Informationssicherheit«, »Datensicherheit« und »IT-Sicherheit« werden im Englischen oft unter dem Oberbegriff



»IT security« oder allgemeiner »information security« zusammengefasst und beschreiben den allgemeinen Schutz von Informationen. Dabei ist es zunächst unerheblich, ob diese Informationen in Form von elektronisch verarbeitbaren Daten oder in Form von Papierdokumenten vorliegen.

Hinweis

Im vorliegenden Buch wird der Begriff »IT-Security« als Oberbegriff des Informationsschutzes in Abgrenzung zum Datenschutz verwendet. Im Fokus liegt dabei vorwiegend der Schutz von Daten, Applikationen und IT-Systemen. Alternativ wird von »Informationsschutz« oder auch »Informationssicherheit« die Rede sein. Alle diese Begriffe werden als Synonyme betrachtet.

1

Das IT-Security-Management hat den Schutz von Know-how im weitesten Sinne zum Ziel. Daraus ist abzuleiten, dass die Sicht rein auf elektronische Daten zu kurz greift, auch wenn dies die Bezeichnung »IT-Security« so suggeriert. Prozesse, Richtlinien und schlicht das Verhalten im Umgang mit Informationen muss so ausgelegt sein, dass der Träger der Information dabei möglichst variabel sein kann. Greift eine Richtlinie in den Prozess des Ausdruckens von Kalkulationstabellen ein, so sind technische Maßnahmen sinnvoll, die es erlauben, sicherzustellen, dass der Ausdruck erst dann geschieht, wenn der berechtigte Mitarbeiter vor dem Drucker steht. Daneben muss es aber auch Richtlinien geben, die festlegen, wie mit den ausgedruckten Tabellen umgegangen werden muss. Zu diesen Vorschriften gehört eine Clean-Desk-Richtlinie genauso wie eine definierte Kennzeichnungspflicht und Regeln bezüglich der Weitergabe dieser Dokumente.

1.7 Selbstverständnis der IT-Security-Organisation

Verantwortlich für das Know-how des Unternehmens in jeder Form ist die Unternehmensleitung. Der Manager IT-Security arbeitet innerhalb des Kompetenzrahmens, der ihm zugewiesen wird, und setzt die Vorgaben und Ziele der Unternehmensleitung zum Informationsschutz um. Sinnvollerweise sind diese Ziele weit gefasst und geben dem Manager IT-Security die Möglichkeit, eigenverantwortlich und umfassend zu agieren. Da anerkanntermaßen



kein 100%iger Schutz möglich ist, wird es immer um eine Annäherung an einen definierten Idealzustand gehen. Dieser Idealzustand bewegt sich zwischen einem optimalen Sicherheitszustand und dem, was mit vertretbarem Aufwand und Kosten möglich ist. Dieser Idealzustand ist das sogenannte »angestrebte Sicherheitsniveau«. Die Annäherung erfolgt in allen Teilbereichen des IT-Security-Managements gleichermaßen, und der jeweilige Status wird immer Schwankungen unterworfen sein.

Wichtig

Die Sicherheitslage zu einem bestimmten Zeitpunkt ist immer eine Momentaufnahme, die schon wenig später anders aussehen kann. Die Herstellung eines Zustands »Sicherheit« ist damit ein Soll-Ziel. Die Aufgabe des IT-Security-Managements ist es, einen Prozess zur Verfügung zu stellen, der kontinuierlich darauf hinarbeitet, das angestrebte Sicherheitsniveau zu erreichen.

1

Der Begriff »Information« umschreibt das schützenswerte Know-how eines Unternehmens und kann in vielerlei Form vorliegen. Dazu gehören Informationen auf Datenträgern genauso wie Konstruktionszeichnungen auf Zeichentischen. Auch wie diese Informationen geschützt werden sollen, ist zumeist anerkanntes Wissen in den Unternehmen und wird durch den Schutz der Vertraulichkeit, der Integrität und der Verfügbarkeit der Informationen umschrieben. Die eben genannten Schutzziele können je nach Bedarf durch weitere ergänzt werden. Ein weiteres Schutzziel, das häufig genannt wird, ist die »Authentizität«. In Abbildung 1.2 werden die gängigsten Schutzziele aufgeführt und kurz beschrieben.

Die Einwirkung der IT-Security beginnt bei der Entstehung der Daten, reicht über deren Verwendung und Weitergabe bis hin zum ordnungsgemäßen, geregelten Löschen. Zu jedem Zeitpunkt innerhalb dieses Lebenszyklus stehen sich die drei Schutzziele in einer Art Spannungsdreieck gegenüber. Zu jedem Zeitpunkt muss also entschieden werden, ob z.B. die Vertraulichkeit leiden darf, um den Grad der Verfügbarkeit für weitere Leser zu erhöhen, oder ob die Integrität der Daten einer gesteigerten Vertraulichkeit weichen darf und die Daten z.B. aus Sicherheitsgründen nicht mehr im Rahmen der Datensicherung gesichert werden.



KAPITEL 1 – UMFANG UND AUFGABE DES IT-SECURITY-MANAGEMENTS

Alle diese Fragen verlangen nach Antworten, die direkten Einfluss auf Informationen, damit auf das Know-how und so wiederum auf die Geschickte eines Unternehmens haben können. Inwieweit die IT-Security regulierend und Entscheidungen treffend in diesen Prozess eingreift, wird von Unternehmen zu Unternehmen unterschiedlich sein und maßgeblich davon abhängen, wie das IT-Security-Management geprägt ist, und vor allem auch, wie es im Unternehmen verankert ist.

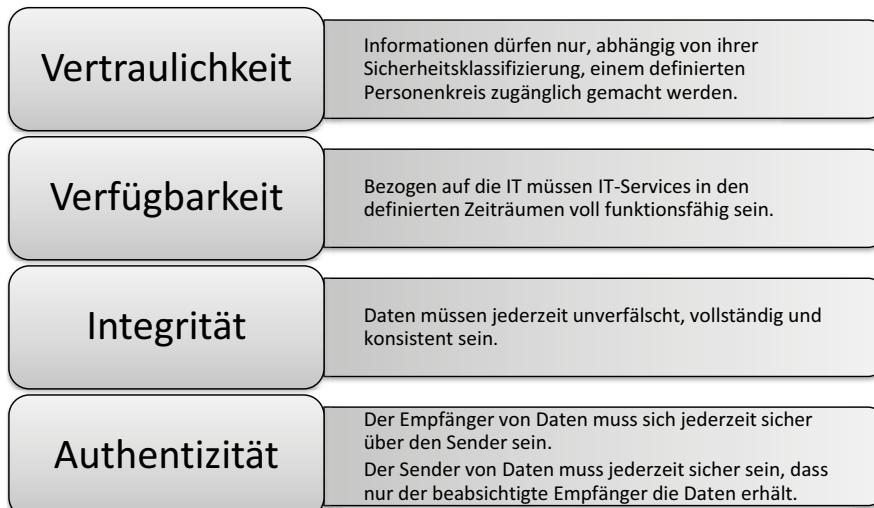


Abbildung 1.2: Schutzziele des IT-Security-Managements

Einer der ersten Schritte beim Aufbau einer IT-Security-Organisation behandelt die Abgrenzung der Aufgaben der IT-Security von den Aufgaben des Dateneigentümers, also des Erstellers der Daten und damit der im Grunde einzigen Person, die den Schutzbedarf einer Information bewerten kann. Ist dieses Verhältnis geklärt und hat das Top-Management eine Aussage darüber getroffen, welchen normativen Grundlagen die IT-Security folgen soll, dann kann damit begonnen werden, die technischen, organisatorischen und rechtlichen Maßnahmen einzuleiten, die erforderlich sind, um die Kernaufgaben zu erfüllen. Was bleibt, ist das oben erwähnte Spannungsfeld und die damit einhergehenden Diskussionen mit den Organisationseinheiten, die jeweils eines der Felder höher priorisieren wollen und die damit in einen Interessenkonflikt mit den Leitlinien der IT-Security geraten können.

Es gibt keine Möglichkeit, diese von Natur aus gegensätzlichen Interessen komplett aufzulösen, und das ist der Hauptgrund dafür, dass ein IT-Security-



Management nicht Bauchentscheidungen folgen darf, sondern formale Methoden entwickeln muss, die dokumentiert sind und durch das Management getragen werden. Durch diese Art der formalen Abarbeitung wird die IT-Security-Organisation weniger angreifbar und damit handlungsfähig bleiben. Wenn die genannten Rahmenbedingungen geklärt sind, die formalen Strukturen existieren und die IT-Security-Organisation mit ausreichenden Kompetenzen ausgestattet ist, kann sie ihre Aufgabe als kontrollierende und regulierende Instanz erfolgreich wahrnehmen.

1.8 Grundregeln

Die allermeisten Handlungen, die im Rahmen der IT-Security auf Basis von Vorgaben, die aus Normen, Regelungen, Verträgen oder auch dem gesunden Menschenverstand abgeleitet wurden, ausgeführt werden, lassen sich auf eine Reihe von grundlegenden Regeln zurückführen, die man oft auch als »Prinzipien« bezeichnet. Diese Regeln werden im Rahmen des vorliegenden Buches an verschiedenen Stellen wieder auftauchen. Die Regeln zu kennen, ist sehr hilfreich, um das »Warum« zu verstehen, wenn innerhalb eines Themenbereichs eine Vorgehensweise beschrieben wird.

1

Regel	Beschreibung
Daten-Informations-eigentümer	<p>Der Ersteller von Informationen (<i>data owner</i>) ist sowohl für deren Sicherheitseinstufung (Klassifizierung) als auch für die ordnungsgemäße Weitergabe der Informationen verantwortlich.</p> <p>Unter dem Risikoeigentümer (<i>risk owner</i>) ist ein Vertreter der Leitung gemeint, der dem Dateneigentümer im Normalfall vorgesetzt ist. Der Risikoeigentümer soll besser als der Dateneigentümer in der Lage sein, den Schutzbedarf der Information einzuschätzen und die erforderlichen Maßnahmen abzuleiten.</p>
Risikoeigentümer	<p>Unter Risikoeigentümer (<i>risk owner</i>) ist ein Vertreter der Leitung gemeint, der dem Dateneigentümer im Normalfall vorgesetzt ist. Der Risikoeigentümer soll besser als der Dateneigentümer in der Lage sein, den Schutzbedarf der Information einzuschätzen und die erforderlichen Maßnahmen abzuleiten.</p>



KAPITEL 1 – UMFANG UND AUFGABE DES IT-SECURITY-MANAGEMENTS

Regel	Beschreibung
Wirtschaftlichkeit	Jede Maßnahme wird auf Wirtschaftlichkeit geprüft, indem ihre Kosten den möglichen Kosten bei Eintritt eines Schadens gegenübergestellt werden. Damit soll vermieden werden, dass mehr Mittel für die Vermeidung eines möglichen Sicherheitsproblems aufgewendet werden, als das Sicherheitsproblem bei Eintritt verursachen würde.
Funktionstrennung (<i>segregation of duties</i> oder auch <i>separation of duties</i>)	Verschiedene kritische Schritte eines Prozesses sollen nicht durch dieselbe Person oder Organisationseinheit wahrgenommen werden. Dies soll sicherstellen, dass nicht eine Person ihre Rechte missbrauchen kann.
1 Vieraugenprinzip (<i>two-man rule</i>)	Sensible Arbeitsschritte sollen nicht durch eine Person umgesetzt werden. So kann z.B. das Passwort für ein kritisches IT-System auf zwei Personen aufgeteilt werden, und der Zugriff auf das System wird in der Folge immer die Anwesenheit beider Personen voraussetzen.
Rechte nach Bedarf (<i>need-to-know</i>)	Jeder Mitarbeiter sollte nur die Zugriffsrechte bekommen, die er für die Durchführung seiner Arbeit benötigt. So haben nur definierte Personen Zugang zu sensiblen Bereichen wie dem Rechenzentrum. Auch der Zugriff auf Daten im Allgemeinen wird nach diesem Prinzip festgelegt.
Weitere Einschränkung von Zugriff und Zugang zu sehr sensiblen Daten und Räumlichkeiten	Auch Personen mit hoher Sicherheitseinstufung bekommen kritische Zugriffsrechte auf bestimmte Daten oder Systeme immer nur zu dem Zeitpunkt und für die Dauer, zu der sie diesen Zugriff benötigen. In dieser Ausprägung handelt es sich um eine Verschärfung der allgemeinen Need-to-know-Regel.
Standardisierung	Das Funktionieren eines IT-Security-Managements setzt die Existenz von Transparenz voraus. Ordnung und Standardisierung von Bezeichnungen, Prozessen oder Installationen sind eine wichtige Voraussetzung, um darauf wiederum standardisierte Sicherheitsprozesse aufsetzen zu können.



Regel	Beschreibung
Poka Yoke	Menschliche, unabsichtliche Fehler führen zu sicherheitsrelevanten Problemen, wie Ausfällen von IT-Systemen oder Fehleingaben. Diese Fehler sind nicht zu 100 % ausschließbar. Die Vorgehensweise nach Poka Yoke (aus dem Japanischen: Poka = Vermeidung, Yoke = unbeabsichtigter Fehler) versucht, durch technische und organisatorische Vorkehrungen die Fehlerrate zu minimieren. Das können Überprüfungsalgorithmen bei der Dateneingabe in Softwaresysteme sein oder ein besseres Eingabe-Interface, das benutzerfreundlicher gestaltet wird.
Datensparsamkeit	Die Datensparsamkeit ist ein Begriff aus dem Datenschutzrecht. Diese Regel besagt, dass es immer vorzuziehen ist, möglichst wenige Daten einer Gefährdung auszusetzen. Besteht die Aufgabe z.B. darin, die Datenübermittlung kritischer Informationen sicher zu gestalten, so ist der erste Schritt der, dafür Sorge zu tragen, dass nur die absolut erforderlichen Informationen übertragen werden.
Privacy by default	Privacy by default legt fest, dass in einem Softwareprodukt, auf einem Betriebssystem oder in einer Firmware schon bei der ersten Inbetriebnahme alle Sicherheitseinstellungen so gewählt sein müssen, dass der Schutz von personenbezogenen Daten maximiert wird.
Privacy by design	Privacy by design bezieht sich auf den Entwicklungsprozess einer Software, eines Betriebssystems oder einer Firmware und legt fest, dass Sicherheitskriterien zum Schutz von personenbezogenen Daten in den verschiedenen Entwicklungsschritten mit einfließen müssen.
Eigenverantwortlichkeit jedes Mitarbeiters	Den Bildschirm zu sperren, wenn ein Mitarbeiter in die Pause geht, oder sensible Informationen nicht auf dem Arbeitsplatz liegen zu lassen, gehören genauso zu den Verantwortlichkeiten eines Mitarbeiters wie der verantwortungsbewusste Umgang mit Daten und Gerätschaften.

Wie die meisten Regeln haben sich auch diese im Laufe der Zeit herausgebildet und wurden schlussendlich als Erforderlichkeit anerkannt. Um allgemeingültig anwendbar zu sein, müssen sie schon per se auf einer höheren



KAPITEL 1 – UMFANG UND AUFGABE DES IT-SECURITY-MANAGEMENTS

Abstraktionsebene angesiedelt sein. Trotzdem fällt es leicht, sich für jedes Prinzip einen Anwendungsfall vorzustellen.

1.9 Umfang des IT-Security-Managements

Das IT-Security-Management ist eine umfangreiche Disziplin, die alle Ebenen und Teilbereiche der IT-Security beinhaltet. Es umfasst zahlreiche technische und organisatorische Aspekte, die bei vielen Gelegenheiten ineinander übergreifen. In Abbildung 1.3 werden viele dieser Aspekte genannt. Eine letztendlich vollständige Übersicht aller Arbeitsgebiete wird sich allerdings erst im Laufe der Ausgestaltung der Arbeit eines jeden einzelnen Managers IT-Security herauskristallisieren.

1

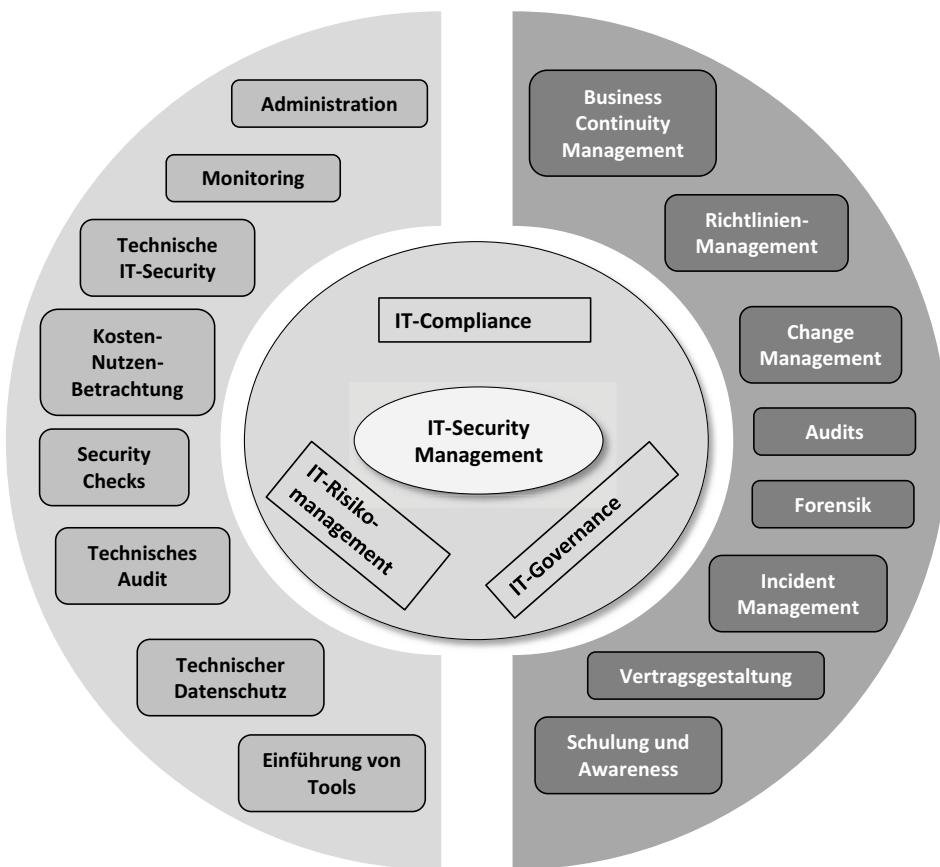


Abbildung 1.3: Aufgabenspektrum des Managers IT-Security



Die Pfeiler des IT-Security-Managements sind die Kernkomponenten IT-Compliance, IT-Risikomanagement und IT-Governance. Sie unterteilen die IT-Security in die drei maßgeblichen Sektoren. Im folgenden Abschnitt wird darauf detaillierter eingegangen. Das Spektrum an Aufgaben, denen sich ein Manager IT-Security stellen muss, ist sehr umfangreich, hat viele Schnittstellen und ist zudem in ständiger Veränderung begriffen. Jede Änderung von Technologien erzeugt automatisch neue Aspekte, die daraufhin in verschiedenen Teilbereichen ihren Niederschlag finden. Auf strategischer Ebene beantworten die Pfeiler der IT-Security die Fragen: »Warum machen wir IT-Security?«, »Wer ist mit IT-Security-Themen befasst?« und »Wie setzen wir IT-Security um?« Wenn diese Fragen beantwortet sind, dann wird sich das weitere Tagesgeschäft in den Teilbereichen abspielen, die im äußeren Kreis in Abbildung 1.3 gezeigt werden.

Jeder Teilbereich hat Schnittstellen zu anderen Teilbereichen, und nur die lückenlose Bearbeitung ergibt einen Sinn. So macht die Erstellung von Richtlinien ohne die Überprüfung im Rahmen von Audits keinen Sinn, die Erstellung von Notfallplänen ohne vorhergehendes Risikomanagement ist uneffektiv, ein Monitoring ohne Mechanismen, auf Ereignisse zu reagieren, ist zwecklos oder die Implementierung von Maßnahmen ohne Feststellung, auf welche Bedrohungen sie eine Antwort finden sollen, ist zielloos. Das stellt die Verantwortlichen vor die Herausforderung, dass es nicht genügt, nur einen Teilbereich zu beherrschen, sondern dass auch die Wechselwirkungen bekannt sein müssen, um im Zweifelsfall die richtige Vorgehensweise wählen zu können.

1.9.1 Pfeiler der IT-Security

Der Aufgabenbereich der IT-Security ist groß, unübersichtlich und wird häufig von verschiedenen Managementstufen aus auch unterschiedlich gesehen. Ein Geschäftsführer will sicher schlafen können, ohne Angst haben zu müssen, dass wichtiges Know-how des Unternehmens bei der Konkurrenz landet. Der Datenschutzbeauftragte benötigt den Manager IT-Security, um effektiv darauf dringen zu können, die technisch-organisatorischen Maßnahmen adäquat umzusetzen. Erst dadurch kann er seinen im Bundesdatenschutzgesetz-Neu formulierten Aufgaben gerecht werden. Für den IT-Leiter ist der Manager IT-Security die Person, die zum einen juristischen und technischen Ärger fernhält, auf der anderen Seite aber auch alle sicherheitsrelevanten Maßnahmen anstößt und lenkt. Für den Budgetverantwortlichen stehen die



KAPITEL 1 – UMFANG UND AUFGABE DES IT-SECURITY-MANAGEMENTS

Kosten im Vordergrund, die auch dann auflaufen, wenn nichts Sichtbares geschieht, die Aufgabe also wirksam verrichtet wird. Diese zahlreichen Anforderungen stehen einer häufig schwammigen Arbeitsplatzbeschreibung entgegen, und dabei den Überblick zu behalten, ist oft nicht leicht. Aus diesem Grund gibt es das IT-Security-Management, das die tragenden Säulen der IT-Security benennt und mit Leben füllt.

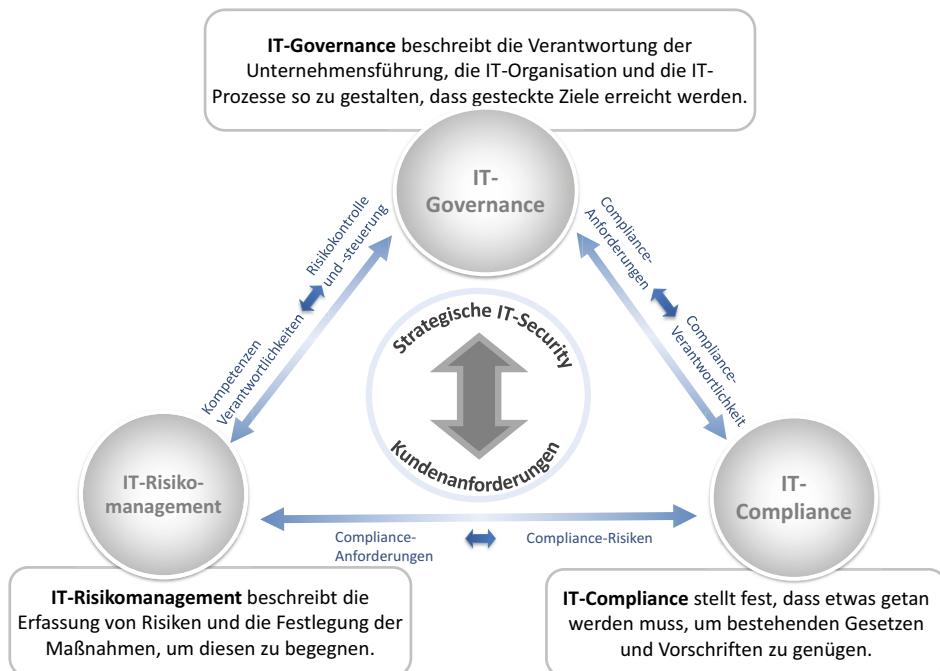


Abbildung 1.4: Spannungsfeld der IT-Security

Drei grundsätzliche Teilbereiche setzt das IT-Security-Management auf strategischer Ebene den eben aufgeführten Schwierigkeiten entgegen:

- das IT-Risikomanagement,
- die IT-Compliance
- und die IT-Governance.

Alle drei Sektoren werden vom Manager IT-Security bearbeitet, sofern sich die Prozesse und Inhalte mit dem Schutz von Informationen beschäftigen. Selbstverständlich haben alle diese Sektoren auch Aspekte, die nichts mit dem Informationsschutz zu tun haben. Diese Aspekte werden entweder völlig



losgelöst oder aber in Verbindung zur Arbeit des Managers IT-Security bearbeitet.

Die Reihenfolge wurde bewusst so gewählt, und es ist gewollt, dass die drei Begriffe als gleichberechtigte Komponenten eines Vorgehensmodells verstanden werden.

Der Manager IT-Security wird sich immer mit diesen drei Sektoren beschäftigen müssen, sofern es keine Organisationseinheiten gibt, die das eine oder andere Feld bereits bearbeiten und auch die Belange der IT-Security mit betrachten. Die jeweilige Gewichtung wird individuell entschieden werden müssen und hängt von vielen Faktoren ab. Zum einen kommt es vor, dass der Manager IT-Security ein bereits existierendes Vorgehensmodell nur modifizieren muss, und zum anderen werden Aufgaben, die z.B. die Verteilung von Aufgaben und Kompetenzen betreffen, außerhalb der IT-Security getroffen und spielen damit direkt in das Feld der IT-Governance hinein. Existiert ein funktionierendes IT-Risikomanagement, angesiedelt z.B. innerhalb des IT-Controllings, dann wird es sinnvoll sein, die dort gelebten Vorgehensmodelle anzupassen oder zu übernehmen. Das Gleiche gilt für das Themengebiet IT-Compliance: Werden die Vorgaben und Regelungen aus Vorschriften oder Gesetzen, die für IT gelten, bereits von einer Rechtsabteilung untersucht, dann wird dies nicht mehr gesondert im Rahmen des Arbeitsplatzes IT-Security erforderlich sein. Die Erfahrung zeigt allerdings, dass dies in den wenigen Fällen zutrifft.

In die richtige Reihenfolge gebracht, beantworten die drei strategischen Sektoren die wichtigsten Fragen der IT-Security. Natürlich wäre es zu kurz gedacht, wenn man die IT-Security darauf beschränken würde. Das liegt schon daran, dass ein Manager IT-Security abhängig davon, in welchem Unternehmensbereich er organisatorisch tätig ist, häufig auch Bereiche bearbeitet, die aus diesem Schema herausragen. Dazu gehören Felder wie das IT-Controlling oder gar die Aufgabe, den Datenschutzbeauftragten zu unterstützen, die immer häufiger mit in das Aufgabenfeld des Managers IT-Security eingebracht werden und weitergehende Qualifizierungen erfordern.

IT-Compliance

Die IT-Compliance beantwortet die Frage: »Was muss getan werden?«

Im Rahmen der IT-Compliance wird definiert, was und warum eine Aufgabenstellung in der IT-Security angepackt werden muss. Dies wird durch eine



KAPITEL 1 – UMFANG UND AUFGABE DES IT-SECURITY-MANAGEMENTS

Vielzahl von Gesetzen, internen Regelungen und die Hauptaufgabe des Schutzes des internen Know-hows festgelegt.

Im Kapitel »IT-Compliance« werden einige, von außen herangetragene Anforderungen exemplarisch aufgeführt, aber sie bilden dennoch nur einen Teil der existierenden Richtlinien ab. Das Spannungsfeld, in dem sich ein Unternehmen befindet, ist äußerst vielschichtig und durch eine undurchschaubar große Anzahl an verzahnten Abhängigkeiten geprägt. Jeder Vertrag mit einem Kunden, jede Änderung der Allgemeinen Geschäftsbedingungen und regelmäßige Gesetzesänderungen führen zu einem Geflecht, in dem es für den Manager IT-Security immer schwieriger wird, die jeweils für die Datensicherheit relevanten Vorgaben zu extrahieren.

1

Wichtig

Im Grunde lässt sich von den einzelnen Anforderungen ein Arbeitsplatzprofil für den Manager IT-Security ableiten. Was nur wieder auf die Grundaussage hinausläuft: Aus dem Bereich der IT-Compliance lässt sich ableiten, was zu tun ist. Da aber vor allem die gesetzlichen Vorgaben schwammig und damit interpretationsfähig sind, ist dieser Anhaltspunkt weniger hilfreich, als zunächst vermutet werden könnte. Aus diesem Grund schaut ein Manager IT-Security neben dem reinen Gesetzestext vor allem auch auf die entsprechenden Gerichtsurteile.

»Compliance« ist eine relativ neue Bezeichnung für ein sehr altes Thema. Schon zu Beginn der Zeiten, als die Großrechner die Rechenzentren in den Unternehmen bevölkerten, war das Thema »Umsetzung von Gesetzen« wie z.B. der Steuergesetzgebung ein Thema. Jahr für Jahr wurden die entsprechenden Lochkarten angepasst und die neuesten Steuerberechnungen elektronisch umgesetzt. Die Personalabteilung war schon in den 1980er Jahren (und in manchen Unternehmen schon Jahre davor) häufiger Gast in den IT-Abteilungen, um die jährlichen Veränderungen Compliance-gerecht umzusetzen. Vor den Computern, zu Zeiten der nichtdigitalen Buchhaltung, war es selbstverständlich in keinster Weise anders. Compliance und im IT-Umfeld die IT-Compliance sind ein sehr altes Thema, das es gibt, seit die ersten Gesetze und Vorschriften entstanden.



Der Tenor der IT-Compliance-Themen der letzten Jahre hat sich verändert. Sie zielen immer mehr direkt auf den Schutz digitaler Daten ab. Im Zuge dieser Modernisierung werden Gesetze ersetzt oder überarbeitet. Diejenigen, die Vorschriften und Gesetze erstellen und in Kraft setzen, arbeiten parallel dazu auch an Methoden, die Umsetzung in den Unternehmen wie auch bei Privatpersonen zu überprüfen. Regelungen ohne Audit führen zu einem Laissez-faire-Verhalten, das sich der moderne Staat nicht leisten will und kann. Die neue Flut an Regelungen und die immer tiefer gehende Überprüfung führten in den letzten Jahren zu einem gesteigerten Bewusstsein aufseiten der Unternehmen für die Wichtigkeit dieses Themas und halfen mit, die Renaissance des Begriffes »Compliance« zu forcieren.

Das kann einer der Gründe sein, warum viele Kommentatoren diesen Sektor als Oberbegriff für das gesamte Thema IT-Security sehen. Gleichgültig, wie man auch zu dieser Aussage steht, eine entscheidende Triebfeder ist sie allemal.

1

IT-Governance

Die IT-Governance beantwortet die Frage: »Wer macht was?«

Die IT-Governance legt fest, wer sich um den Informationsschutz kümmern muss und welche Kompetenzen er dafür erhält. Die Delegation dieser Aufgabe bis hin zur organisatorischen Umsetzung im Unternehmen gehört zu diesem Teilgebiet. Das Wort Governance bedeutet »Regierung« oder »Steuerung«. Daraus wird ersichtlich, dass sie alle steuernden und kontrollierenden Instrumente im Umfeld der IT beinhaltet.

Ein Manager IT-Security, vor allem in einem großen Unternehmen, wird immer von der Hilfestellung lokaler IT-Einheiten abhängig sein. Liegt die Kernkompetenz des Managers IT-Security im formalen Bereich, so wird er Unterstützung bei technischen Fragen benötigen. Liegt die Lage andersherum und der Manager IT-Security kommt originär aus dem technischen Umfeld, so wird er unter Umständen Hilfe bei Juristen oder im Controlling anfragen müssen, um seine Aufgaben, die eher dort angesiedelt sind, abarbeiten zu können. Ein gutes Netzwerk zu allen zutragenden organisatorischen Einheiten ist wichtig. Genauso wichtig ist, dass der Manager IT-Security bei allen diesen Fragen als zuständige Person definiert wird.



KAPITEL 1 – UMFANG UND AUFGABE DES IT-SECURITY-MANAGEMENTS

Wie auch immer das Netz an innerbetrieblichen Abhängigkeiten gestaltet sein mag, eine genaue Festlegung von Kompetenzen und Verantwortlichkeiten ist ein wichtiger Schlüssel zum Erfolg.

IT-Risikomanagement

Das IT-Risikomanagement beantwortet die Frage: »Wie wird es umgesetzt?«

Zu guter Letzt gibt das IT-Risikomanagement die Antwort darauf, wie es zu tun ist. Der gesamte Risikomanagementprozess dient letztendlich dazu, Schwachstellen zu finden, zu quantifizieren und entsprechende, abgewogene Maßnahmen als Antwort darauf zu finden. Zudem beantwortet das IT-Risikomanagement die Frage, ob eine Vorgehensweise finanziell angemessen ist, in welchem Bereich eher investiert werden sollte und ob ein Risiko im Zusammenhang mit einem Prozess, Projekt oder einer Aufgabe aus Sicht der Risikoabwägung tragbar ist oder nicht.

Steht ein Manager IT-Security vor der Frage, ob eine Firewall abgeschaltet werden muss, weil ein Trojaner von außen bestimmte Systeme penetriert, die Abschaltung aber wiederum Kosten in der Produktion generieren würde, so kann diese sinnvoll nur auf einer formalen Risikoeinschätzung basieren. Die IT-Compliance wird die gesetzliche und auf internen Vorgaben beruhende Grundlage bilden und die IT-Governance die Frage nach den vorhandenen Kompetenzen beantworten.

1.9.2 Aufgaben des IT-Security-Managements

Das IT-Security-Management beantwortet unter anderen die Fragen »Sind die eingesetzten Maßnahmen und Prozesse effektiv?« und »Wie ist die aktuelle Sicherheitslage?« zu einem beliebigen Zeitpunkt. Um dies bewerkstelligen zu können, ist der IT-Security-Kreislauf innerhalb des Information-Security-Management-Systems (ISMS) zu etablieren und zu betreiben. Dazu steuert der Manager IT-Security die Abarbeitung der verschiedenen Aufgaben der IT-Security wie das IT-Risikomanagement, technische Maßnahmen, die Überwachung von Systemen und Applikationen oder das Business Continuity Management und das IT-Notfallmanagement. Einen Überblick über die Tätigkeitsfelder gibt Abbildung 1.5.

Die IT-Compliance stellt dabei den Rahmen dar, innerhalb dessen sich das IT-Security-Management generell bewegt. Das IT-Risikomanagement stellt die



UMFANG DES IT-SECURITY-MANAGEMENTS

Methodik zur Verfügung, mit deren Hilfe eine Bewertung von Aufgaben und die Definition entsprechender Maßnahmen möglich werden. Alle aufgeführten Bereiche der IT-Security unterliegen wiederum dem Regelkreislauf des IT-Security-Managements, sprich: Alle müssen regelmäßig auf ihre Wirksamkeit überprüft, angepasst und überwacht werden. Dazu kommt, dass laufend neue Bereiche zu identifizieren sind, die in ein IT-Security-Management integriert werden müssen.

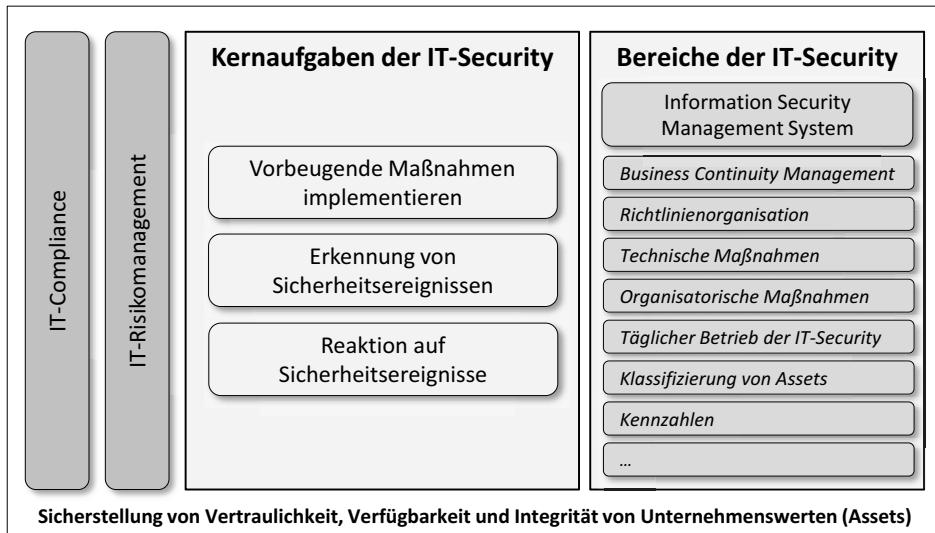


Abbildung 1.5: Aufgaben des IT-Security-Managements

Der Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Daten, IT-Systemen und damit von Services und Geschäftsprozessen verlangt einen hohen Grad an geregelten Vorgaben innerhalb der IT genauso wie in den Fachabteilungen. Bevor Maßnahmen zum Schutz der Unternehmenswerte umgesetzt werden können, bedarf es entsprechender Richtlinien. Bevor ein Mitarbeiter mit diesen umgehen kann, sind Schulungen und Anweisungen erforderlich. Um wissen zu können, welche IT-Systeme vorrangig zu schützen sind und für welche IT-Systeme entsprechende Finanzmittel zur Verfügung gestellt werden müssen, sind umfangreiche Erhebungen im Rahmen eines IT-Risikomanagements erforderlich. Alle diese Punkte basieren wiederum auf möglichst detaillierten Aufzeichnungen über den aktuellen Stand der IT, dargestellt unter vielen anderen Dokumenten in Netzwerkplänen, im Assetmanagement, in der Anlagenbuchhaltung, auf Wartungsplänen oder in



KAPITEL 1 – UMFANG UND AUFGABE DES IT-SECURITY-MANAGEMENTS

Prozessübersichten. Davon ausgehend, dass im Rahmen eines umfassenden Business-Continuity-Plans auch Maßnahmen zur Aufrechterhaltung des IT-Betriebs ergriffen werden müssen, fließen alle diese Informationen letztendlich wieder in Notfallpläne und Wiederherstellungsmaßnahmen.



1

Abbildung 1.6: Steuerungsfunktion

Da niemand einer Dokumentation Glauben schenkt, die ein gewisses Alter (in vielen Fällen fängt dies bei wenigen Monaten an) überschritten hat, kann auch ein IT-Leiter nur dann beruhigt schlafen, wenn er weiß, dass alle eben genannten Pläne, Dokumente, Datenbanken, Risikoübersichten, Terminpläne oder Wartungspläne innerhalb eines kontinuierlichen Verbesserungsprozesses laufend untersucht, angepasst und verbessert werden. Allein um die letzten Punkte überprüfen zu können, ist ein weiterer Baustein, das Audit, erforderlich.

Die Aufgabenfelder eines IT-Security-Verantwortlichen sind vielfältig und eng vernetzt mit den Aufgaben der IT und vieler anderer Fachabteilungen. Auf den ersten Blick ist zudem erkennbar, dass die klassischen technischen Bereiche eher formal bürokratischen weichen.

Der heutige Manager IT-Security werkelt nicht mehr abgeschottet am Terminal und löst Sicherheitsfragen auf niedrigen Ebenen des TCP/IP-OSI-Modells, sondern er kommuniziert, moderiert und entwirft Szenarien, die wiederum in Regelungen münden. Das IT-Security-Management umfasst alle Bereiche, und zwischen ihnen zu jonglieren, ohne dabei den Blick in die direkt betroffenen Unternehmensbereiche zu verlieren, ist dessen Hauptaufgabe.



In dem Maße, wie der Abstand zur Technik wächst, muss die Zusammenarbeit mit den technischen Spezialisten in der IT zunehmen. Technische Bewertungen und Lösungen müssen delegiert werden, ohne dass der Gesamtüberblick bis ins Detail völlig verloren geht.

Die Steuerungsfunktionen des IT-Security-Managements, wie sie in Abbildung 1.6 abgebildet sind, dienen dazu, auf Ereignisse richtig zu reagieren, die Erkenntnisse zu bewerten und daraus zu lernen. Außerdem müssen mitbeteiligte Organisationseinheiten informiert, geschult und letztendlich auch angewiesen werden, im Sinne der Ziele der IT-Security zu agieren.

1.10 IT-Security zwischen Nutzen und Kosten

Der Manager IT-Security ist in allererster Linie ein Moderator, der zwischen den Stühlen Kosten, Kundenanforderungen und den Sicherheitsbelangen sitzt. Zum inneren Spannungsfeld von IT-Governance, IT-Compliance und IT-Risikomanagement kommen äußere Ansprüche hinzu, die sich zumeist nicht vollständig auflösen lassen. Zunächst einmal ist der Grund darin zu suchen, dass die IT-Security keinen einfach nachzuweisenden ROI leistet. Häufig kommt hinzu, dass die IT-Security eher als verhindernde denn als unterstützende Organisationseinheit gesehen wird. Das ist auch der Grund, warum ein Arbeiten in diesem Umfeld ohne Rückhalt aus der Unternehmensleitung ineffizient und schwierig ist.

Findet ein Angriff auf Unternehmensdaten statt, von innen oder von außen, und wird dieser professionell und zielgerichtet ausgeführt, dann wird nur ein Bruchteil der Unternehmen diesen überhaupt bemerken. Je größer ein Unternehmensnetzwerk ist, je mehr Personen Zugriff auf geheime Daten haben und je sorgloser mit ihnen umgegangen wird, desto leichter wird es einem Angreifer gemacht. Dazu kommt der schleichende Verlust von Daten als ein weiteres Phänomen. Dies geschieht über unverschlüsselte E-Mails, unverschlüsselte Dateiübertragung oder Papiermüll, der auch sensible Daten enthält. Alle Kommunikationswege lückenlos zu überwachen, stellt eine schier unmögliche Aufgabe dar. Selbst wenn dies technisch gelöst wird, scheitern Unternehmen reihenweise daran, die erfassten Überwachungsdaten zu analysieren und daraus die korrekten Schlüsse zu ziehen. Alle diese Gründe erfordern ganz offensichtlich den Einsatz von Maßnahmen aus dem IT-Security-Umfeld. Da aber eine objektive Abwägung zwischen den damit auflaufenden



KAPITEL 1 – UMFANG UND AUFGABE DES IT-SECURITY-MANAGEMENTS

den Kosten und dem zu erzielenden Nutzen nicht durchgeführt werden kann, wird häufig an den falschen Stellen oder zu wenig investiert.

Die Business-Impact-Analyse hat die Aufgabe, eine Kostenschätzung für den Fall zu erstellen, dass wichtige Kernprozesse im Unternehmen ausfallen. Die daraus abgeleiteten Ergebnisse stellen die wichtigsten Kenngrößen für den Nutzen dar, den die Sicherstellung von Verfügbarkeit, Vertraulichkeit und Integrität für das Unternehmen wirklich bringt. Es findet dabei eine Betrachtung für den Fall statt, dass etwas ausfallen könnte, und fällt damit in den Bereich der Versicherung gegen mögliche Notfälle. Wie jede Versicherung können diese Daten für eine Risikoabwägung herangezogen werden, aus der die Finanzmittel rechnerisch hervorgehen, die sinnvollerweise in die Notfallvorsorge investiert werden sollten.

1

Im Gegensatz zu einer Versicherung gegen Notfälle ist es erforderlich, den tatsächlichen Nutzen einzelner Maßnahmen zu überprüfen. Für diesen Zweck sind Kennzahlen wünschenswert, um eine Situation quantitativ vor und nach der Umsetzung einer Maßnahme bewerten zu können. Nachdem Einigkeit besteht, dass eine Messung des Nutzens von IT-Security vorgenommen werden soll, müssen zunächst der Rahmen der Messung und die Art der Messmethode festgelegt werden. Um messen zu können, müssen Prozesse gefunden werden, die messbar sind. Entscheidet man sich z.B. für den Prozess »Mailversand nach extern«, dann würde der nächste Schritt so aussehen, dass alle Quellen für Daten wie Logfiles zusammengetragen und daraufhin untersucht werden, ob sie tauglich sind. Ein Beispiel wäre in diesem Fall die Anzahl von Viren, die die Mailkette passieren und bis zum Zielrechner gelangen. Standardwerte aus dem täglichen Betrieb des Mailsystems werden später als Kontrolldaten dienen. Vergleichswerte von anderen Unternehmen können dazu dienen, das eigene Unternehmen einzuschätzen. Nach der Umsetzung von Maßnahmen wird die Kontrollmessung zeigen, ob die Anzahl an Viren niedriger geworden ist. Aus der Gegenüberstellung der Kosten für die implementierte Maßnahme und der Ersparnis aus einer niedrigeren Zahl an Viren, die den Rechner des Empfängers infizieren könnten, ergibt sich der Nutzen.

Das Beispiel zeigt, dass auf der einen Seite eine lückenlose Darstellung des Nutzens von IT-Security schwierig und kostenintensiv ist, auf der anderen Seite die Messung des Erfolgs eingeführter Maßnahmen aber eine wichtige Aufgabe darstellt, insbesondere was die Darstellung eines verringerten oder auch erhöhten Risikos angeht.



2 Organisation der IT-Security

2.1 Kapitelzusammenfassung

In einem Unternehmen verteilt sich die vielfältige Aufgabe des Schutzes von Unternehmenswerten auf eine ganze Anzahl von Rollen. Diese Rollen stehen in einem Verhältnis zueinander, das der Manager IT-Security kennen und mitgestalten sollte. Innerhalb dieses Kapitels werden die wesentlichen Rollen aufgezeigt und mögliche Arbeitsinhalte beschrieben.

Die Top-5-Fragen zum aktuellen Kapitel:

- Wurde die Rolle des Managers IT-Security offiziell implementiert?
- Ist die Rolle des Managers IT-Security innerhalb der Organisationsstruktur offiziell veröffentlicht worden?
- Sind die für die Arbeit eines Managers IT-Security erforderlichen Kompetenzen eingeräumt und definiert worden?
- Wurde der Aufgabenbereich des Managers IT-Security gegenüber den anderen Stellen, die sich um Sicherheitsbelange kümmern, ausreichend abgegrenzt?
- Sind die Kommunikationswege zwischen den verschiedenen Sicherheitsbereichen, von denen der Manager IT-Security eine repräsentiert, definiert?

2.2 Einführung

Die IT-Security-Organisation ist nicht nur erforderlich, um die tägliche Arbeit und die Verantwortlichkeiten für das Arbeitsgebiet zu strukturieren. Sie ist zudem ein Ausdruck der Unternehmensleitung, inwieweit der Gesamtthematik »Datensicherheit« Aufmerksamkeit geschenkt wird. Deshalb kann aus der Art und Weise, wie die Organisationseinheit IT-Security aufgebaut ist, ablesen werden, mit welcher Priorität der Informationsschutz betrieben wird. Ist der Manager IT-Security einer IT-Abteilung zugeordnet, so wird seine Weisungsbefugnis nicht so weitreichend sein, als wenn er direkt dem Vorstand untergeordnet ist. Ist er global aufgestellt, also für alle Unternehmensteile



bzw. auch im Ausland zuständig oder gibt es für jede Ländergesellschaft einen eigenen? Hängt er am Datenschutzbeauftragten oder arbeitet er eng mit diesem zusammen? Die Beantwortung dieser Fragen lässt direkte Rückschlüsse zu und das sollte angemessen berücksichtigt werden.

Die Struktur der IT-Security ist damit auch ein Aushängeschild nach außen. Damit kann Kunden aufgezeigt werden, wie ernst der Schutz ihrer Daten genommen wird. Das wiederum kann dazu führen, dass innerhalb des Unternehmens eine Struktur geschaffen wird, die nur repräsentativen Charakter hat und im Grunde nicht wirklich gelebt wird. Diese Ausprägung kommt häufiger vor, als man zunächst vermuten würde, und birgt die Gefahr, dass sich die Verantwortlichen im Unternehmen beruhigt auf die Schultern klopfen, ohne wirklich Sicherheit geschaffen zu haben. Aus diesem Grund ist nicht nur der Aufbau einer Organisationseinheit das Ziel, sondern auch die Ausstattung mit Ressourcen wie Mitarbeitern, Zeit und Budget, und die zugewiesenen Kompetenzen müssen stimmen.

2

2.3 Rollen innerhalb des IT-Security-Managements

Je vielschichtiger und vielfältiger die Aufgabenbereiche der IT-Security werden, desto mehr spezialisierte Berufsfelder bilden sich innerhalb dieser Thematik heraus. Kam der Manager IT-Security früher zumeist direkt aus dem administrativen Bereich der IT und beschäftigte er sich deshalb auch maßgeblich mit den technischen Aspekten, so kamen mit den Feldern IT-Compliance und IT-Risikomanagement bald neue Aufgaben hinzu, die Kenntnisse in ganz anderen Disziplinen erforderlich machten. Das bedeutet nicht, dass sich die verschiedenen Rollen nicht in einer Person konzentrieren können. Zumindest aber muss dieser Person bewusst sein, dass es diese Rollen gibt und dass es erforderlich ist, auch diese gegenüber den Kollegen, Vorgesetzten und externen Prüfern zu vertreten. So wird der Manager IT-Security von einem Wirtschaftsprüfungsunternehmen anders wahrgenommen als von einem Kollegen aus der IT, der ein Problem mit einem Sicherheitspatch hat: eine Person in zwei gänzlich unterschiedlichen Rollen.

2.3.1 Manager IT-Security

»Manager IT-Security«, »Chief Information Security Officer (CISO)« oder »Leiter Informationsschutz« wird die Rolle genannt, die für das IT-Security-



ROLLEN INNERHALB DES IT-SECURITY-MANAGEMENTS

Management verantwortlich zeichnet. Das bedeutet nicht, dass der Manager IT-Security in letzter Instanz für den Schutz der Informationen verantwortlich ist. Diese Verantwortung liegt weiterhin bei der Unternehmensleitung. Das liegt in der Natur der Rolle eines Geschäftsführers begründet. Zudem ist der Schutz der Informationen Teil der unternehmerischen Verantwortung und kann nicht ohne Weiteres delegiert werden. Die Unterscheidung zwischen dem Betreiben eines IT-Security-Managements, also dem Ausfüllen eines Jobs, und der generellen Verantwortung für die Sicherheit des Unternehmens-Know-hows ist wichtig und sollte immer im Hinterkopf behalten werden. Sie ist auch ein Grund dafür, warum die grundlegenden Entscheidungen wie die Verabschiedung einer Sicherheitsrichtlinie immer Aufgabe der Unternehmensleitung ist.

Im Idealfall ist der Manager IT-Security für die unternehmensweite Organisation der IT-Security zuständig und erhält seinen Auftrag aus der IT, der Unternehmensleitung direkt, vom Datenschutzbeauftragten oder in selteneren Fällen aus einer weiteren Fachabteilung wie z.B. der Rechtsabteilung oder dem Controlling. Der ideale Umfang des Zuständigkeitsbereichs hängt von vielen Faktoren ab. Ein technischer Faktor ist die Struktur des Unternehmensnetzwerks. Ist dieses flach und verbindet es alle Unternehmensteile gleichermaßen, dann macht es wenig Sinn, den Scope auf Teilbereiche einzuschränken. Besteht das Unternehmen jedoch aus vielen Einzelgesellschaften mit jeweils eigener IT-Infrastruktur und Firewalls, die jeden Einzelbereich abschotten, dann kann es auch sinnvoll sein, diese Aufgabe zu teilen, solange das einzuhaltende Mindest-Sicherheitsniveau flächendeckend vergleichbar hoch ist.

Ein weiterer Faktor ist wiederum die Außenwirkung. Die Implementierung der Funktion IT-Security erfolgt häufig aus der Erforderlichkeit heraus, externe Anforderungen bezüglich der Sicherstellung des Betriebs zu gewährleisten und auch nachweisbar zu gestalten. Dafür ist die Konzentration dieses Aufgabengebiets in einem Bereich förderlich, um die dazugehörigen Steuerungsfunktionen wahrnehmen zu können.

Unternehmen, die die Funktion Security als zusätzliche Aufgabe den Fachverantwortlichen der verschiedenen IT-Bereiche zuordnen, stehen bald vor dem Problem, dass eine Abstimmung schwierig und ein standardisiertes Vorgehen fast unmöglich wird. In einem Unternehmen mit zehn Standorten würde das bedeuten, dass der jeweilige lokale Support sich um die Client-Sicherheit kümmert, der lokale Netzwerkverantwortliche um die Sicherheit seiner Netz-



KAPITEL 2 – ORGANISATION DER IT-SECURITY

werkkomponenten und die lokal angesiedelten Administratoren um den Rest. Ohne zentrale Steuerung wird die Streuung des Sicherheitsniveaus zwischen den Lokationen stark von den jeweiligen Fachkenntnissen der Mitarbeiter abhängen. Ohne zentrale Überprüfung und Steuerung stellt dies ein großes Sicherheitsproblem dar.

Hinweis

Ohne eine unternehmensweit agierende Organisationseinheit IT-Security mit einem verantwortlichen Manager IT-Security wird das Sicherheitsniveau von Standort zu Standort stark schwanken. Das Gesamtniveau wird auf das Niveau des schwächsten Standorts sinken, und die Umsetzung standardisierter Verfahren wird stark behindert.

2

Nicht zuletzt stellt es einen Wettbewerbsvorteil dar, ein IT-Security-Management dediziert zu betreiben. Das liegt zum einen daran, dass dadurch leichter nachzuweisen ist, dass sicherheitsrelevante Informationen von Kunden und Lieferanten regelkonform verarbeitet werden, und des Weiteren wird das eigene Know-how geschützt. Unternehmen, die in der Öffentlichkeit präsent sind wie Kreditkartenunternehmen oder Webmail-Provider, werden in viel höherem Maße auf das Vorhandensein einer solchen Stelle geprüft werden als kleine Betriebe mit nicht allzu komplexer Entwicklungstätigkeit und weniger Konkurrenzdruck. Das Gleiche gilt für Unternehmen, die kritische Infrastrukturen betreiben. Diese Unternehmen fallen unter das im Juni 2015 verabschiedete IT-Sicherheitsgesetz und werden darin verpflichtet, die für die Erbringung ihrer wichtigen Dienste erforderliche IT nach dem Stand der Technik abzusichern. Diesbezüglich fällt dem Manager IT-Security eine weitere Rolle zu: Er ist nach außen hin die Person, die die Sicherheit der Kundendaten und der IT-Infrastruktur auf technischer Ebene sicherstellt. Dies wiederum gewährleistet er durch die Einführung und den Betrieb entsprechender Regeln und Prozesse. Damit ist er der erste Ansprechpartner für Nachfragen, Besorgnisse und die Kommunikation, falls etwas schiefläuft oder der Kunde diesen Bereich auditiert.

Der Manager IT-Security grenzt sich in seiner Funktion ganz bewusst von anderen Sicherheitsfunktionen wie z.B. dem Verantwortlichen für den Objektschutz ab. Das ist ein Beispiel dafür, dass nicht alle Felder der Unternehmens-



ROLLEN INNERHALB DES IT-SECURITY-MANAGEMENTS

sicherheit direkt mit der Informationstechnologie verbunden sind und es damit zu sich überschneidenden Zuständigkeiten kommen kann. Der eben angesprochene Verantwortliche für den Objektschutz ist für den Zutritt zu Gebäuden verantwortlich. Dazu gehören auch Bereiche, in denen Prototypen gelagert werden. Diese wiederum gelten als wichtige, zu schützende Werte, für die ein Manager IT-Security im Normalfall nicht zuständig sein wird, obwohl sie auch eine Art Information darstellen. Also muss es dafür eine weitere Stelle geben, die eng mit diesem zusammenarbeiten muss. Noch deutlicher wird es, wenn es um Rechenzentren geht. Dabei handelt es sich wieder um zu schützende Räumlichkeiten, für deren Zutrittsschutz der Objektschutz zuständig sein wird und die die IT erst übernimmt, wenn es um das Innere der Räume geht. Diese Beispiele sollen aufzeigen, dass eine Berufsbezeichnung noch lange nicht den Inhalt und den Umfang des tatsächlichen Tätigkeitsfelds definiert. Wenn keine wichtigen Aufgaben vergessen werden sollen, dann kann man anhand der verschiedenen Normen jedem darin behandelten Thema eine Rolle zuordnen und die Wechselbeziehungen zwischen ihnen definieren.

Hilfreich ist zudem ein Blick in aktuelle, typische Stellenanzeigen, die den Job eines Managers IT-Security oder generell eines IT-Security-Experten beschreiben:

- Die Jobbezeichnung entwickelt sich allmählich weg von der deutschen Bezeichnung »Leiter Informationsschutz«, und immer häufiger ist von einem »Manager IT-Security« die Rede, wenn es um eine leitende Stellung geht, und von einem »IT-Security-Manager«, »IT-Security-Experten« oder »IT-Security-Spezialist«, im Englischen »IT-Security Professional«, wenn es um die Mitarbeit in einem Team geht. Der Titel »Chief Information Security Officer« (CISO) ist vor allem in Unternehmen anzutreffen, die international aufgestellt sind und auch dementsprechend international rekrutieren. Ein weiterer Titel, der sich langsam durchsetzt, ist der des »Managers Cyber Security«. Bislang war das Tätigkeitsfeld eines Cyber-Experten beschränkt auf die Abwehr von Gefahren aus dem Internet. Mit der Erweiterung der Aufgaben auf die Sicherung aller Arten von Datenübermittlungen erweitert sich auch das Aufgabengebiet, das diesem Begriff zugeordnet wird.
- Das Aufgabengebiet »IT-Security-Management« oder »Information-Security-Management« wird immer häufiger explizit genannt und deutet an,



KAPITEL 2 – ORGANISATION DER IT-SECURITY

dass neben der technischen Implementierung von Applikationen auch die Implementierung von Prozessen zur täglichen Routine gehört. Die Weiterentwicklung der IT-Security-Strategie ist dabei das langfristige Ziel. Analog zum IT-Security-Management werden auch der Aufbau und die Weiterentwicklung eines »ISMS«, also eines »Information-Security-Management-Systems« nach ISO 27001, genannt.

- Die Identifizierung von Risiken und die darauf folgende IT-Risikobehandlung, die häufig direkt im Zusammenhang mit den BSI-Standards oder den entsprechenden ISO-Normen genannt werden, rücken immer häufiger an die erste Stelle der Anforderungsliste. Diese Punkte stellen die Basis des modernen IT-Security-Managements dar. Die Verwaltung und Behandlung von Risiken, die sich aus dem IT-Betrieb heraus ergeben, werden in diesem Zug an die IT-Security-Organisation weitergereicht.
- Die Einführung bzw. Pflege einer Richtlinienstruktur und die darauf aufbauende Überprüfung des Sicherheitsniveaus in Form von Audits und dem Monitoring ist ein weiterer Baustein, der im Anforderungsprofil ganz weit oben angesiedelt ist. In diesem Zusammenhang werden regelmäßig die rechtlichen Rahmenbedingungen aufgeführt, die für das Unternehmen von Belang sind. So werden im Rahmen von Qualitätsaudits immer detailliertere Fragen nach der IT-Security gestellt genauso wie bei der Zertifizierung nach C-TPAT bzw. der europäischen Variante AEO, wenn es um die Logistik geht. Für Zulieferer in der Automobilindustrie wiederum sind die Audits auf Basis TISAX (steht für »Trusted Information Security Assessment Exchange«), wie sie durch den Verband der Automobilindustrie (VDA) definiert werden, wegweisend. Im Grunde folgen alle diese Audits der ISO-27002-Norm und der Beschreibung eines IT-Security-Management-Systems nach ISO 27001, so wie sie im vorliegenden Buch beschrieben ist.
- Das IT-Notfallmanagement ist ein Punkt, der als unterstützende Funktion beschrieben wird. Unterstützt wird dabei die IT oder auch das Gebäude-Management in der Entwicklung und Pflege entsprechender Prozesse und Dokumentationen. In der Praxis zeigt sich allerdings, dass das Know-how sehr häufig eher vonseiten geschulter Manager IT-Security kommt als von IT-Mitarbeitern. Dieser Trend scheint sich in dem Maß zu verstärken, in dem ein Manager IT-Security auch in Fragen der IT-Compliance ausgebildet sein muss und sich schon deshalb mit den entsprechenden Dokumenten vertraut gemacht hat.



ROLLEN INNERHALB DES IT-SECURITY-MANAGEMENTS

- Eine enge Verzahnung des Managers IT-Security mit dem Bereich, der sich um den Datenschutz kümmert, ist heute selbstverständlich, und zumindest rudimentäre Kenntnisse der Datenschutzgesetze sind eine weitere Herausforderung, der sich der Manager IT-Security heute stellen muss.
- Die Schulung von Mitarbeitern und das Vorantreiben der allgemeinen Awareness, was den Bereich IT-Security angeht, schließt viele Stellenbeschreibungen ab, ein Gebiet, das sehr individuell gehandhabt werden muss und das deshalb auch selten weiter ausgeführt wird.

Zudem wird sehr deutlich, dass ein Manager IT-Security als eine Person verstanden wird, die berät: entweder die IT in technischen Funktionen, den Fachbereich in Abläufen oder Entscheidungsträger hinsichtlich der Risikoeinschätzungen.

2

Wichtig

Ein Berater wird immer eine Aufgabe haben, die einem steten Wandel unterworfen ist und dessen Umfang wachsen wird. Die Regel, die sowieso schon für jeden Mitarbeiter in einem technischen Beruf gilt, dass im Laufe des Arbeitslebens das Hinzulernen von immenser Wichtigkeit ist, gilt in ganz besonderem Maße auch für einen Mitarbeiter innerhalb der IT-Security-Organisation.

In seiner Steuerungsfunktion werden einem Manager IT-Security zumindest kurzfristige Befugnisse zugewiesen, die großen Einfluss auf Prozesse innerhalb und außerhalb des Unternehmens haben. Diese werden vorwiegend in Ausnahmesituationen relevant. Dazu gehören Notfälle im Rahmen des IT-Notfallmanagements wie der Ausfall von Systemen oder Situationen, die einen Ausfall nach sich ziehen könnten, z.B. ein akuter Angriff durch Angreifer von außen. Im letzteren Fall könnte die Entscheidung im Raum stehen, den Zugang zum Internet zu kappen, um einem Angreifer den Weg ins interne Unternehmensnetzwerk zu versperren. Eine solche Vorgehensweise zieht viele Konsequenzen nach sich. Dazu gehören die Verbindungen zu Außenstellen per Internet-VPN oder der Zugriff auf Unternehmensdaten durch Kunden und Lieferanten, die in einem solchen Fall auch nicht mehr funktionieren würden. Tritt ein solcher Fall ein, hat der Manager IT-Security die zentrale Funktion, den letztendlichen Entscheider zu beraten und eine



Entscheidung zu forcieren, oder er vereinigt in seiner Rolle auch die Befugnisse, eine solche Abschaltung selbst anzuweisen.

2.3.2 Unternehmensleitung

Der Schutz von Unternehmensdaten ist eine originäre Aufgabe der Unternehmensleitung. Dies leitet sich nicht nur aus der logischen Erforderlichkeit der Fortführung des Geschäftsbetriebs, sondern auch aus verschiedenen gesetzlichen Regelungen ab.

Je mehr ein Unternehmen von seinem technischen Know-how abhängig ist, desto höher ist auch der potenzielle Schaden, den ein Angriff oder ein Systemausfall verursachen kann. Daraus leitet sich auch ab, wie engmaschig ein IT-Security-Management gestaltet werden muss und welche Unternehmensteile primär zu betrachten sind.

Die Unternehmensleitung legt in einem grundlegenden Schritt die Sicherheitsstrategie im Rahmen der Sicherheitsrichtlinie fest und definiert dadurch die Leitplanken, zwischen denen sich das IT-Security-Management bewegt. Dabei sind Rahmenbedingungen aus gesetzlichen und anderen Vorgaben zu beachten. Unter »andere Vorgaben« fallen z.B. alle Vorgaben, die ein Kunde in seinen Verträgen festlegt.

Ist die Aufgabe des IT-Security-Managements definiert, dann legt die Unternehmensführung die Sicherheitsorganisation fest. Dazu gehört die Einordnung in die Unternehmensorganisation und eine Beschreibung aller Berichtswege. Ein weiterer Punkt ist die Beschreibung der Kompetenzen der IT-Security-Organisation innerhalb des Unternehmens. Ausgestattet mit Kompetenzen und im Unternehmen verankert kann daraufhin eine Zielvereinbarung abgeschlossen werden, was die gegründete Einheit im Rahmen der Ziele des Unternehmens und, enger gefasst, im Rahmen der Datenverarbeitung leisten soll.

2.3.3 Weitere Rollen

Besteht das gesamte IT-Security-Team in kleinen Firmen häufig aus einer einzelnen Person, die dieses Thema zumeist auch nur in einem Bruchteil ihrer Arbeitszeit bearbeitet, so stehen großen Unternehmen ganz andere Ressour-



ROLLEN INNERHALB DES IT-SECURITY-MANAGEMENTS

cen zur Verfügung. Verschiedene Teilbereiche werden dabei auf verschiedene Rollen verteilt, die häufig dediziert Personen zugeordnet werden.



Abbildung 2.1: Rollen innerhalb der IT-Security-Organisation

Die Rollen »Manager IT-Security«, »IT-Security Professional«, »IT-Risikomanager«, »Manager IT-Compliance« und »IT-Security-Auditor« lassen sich direkt dem IT-Security-Management zuordnen, während Rollen aus der IT, wie die des Administrators der Firewall, als unterstützende, aber trotzdem essenzielle Rollen zu sehen sind.

Neben den genannten Rollen kann es natürlich noch weitere geben, und je nachdem, wo in der Zukunft die Schwerpunkte gesehen werden, wird sich auch deren Gewichtung weiter verändern. So ist heute schon der »Compliance Manager« in Banken und Versicherungen weit häufiger anzutreffen als im produzierenden Gewerbe, und es ist dort nicht selten der Fall, dass diese Rolle die Gesamtverantwortung für die IT-Security-Organisation innehat.



2.4 Verankerung im Unternehmen

Nach innen und nach außen zu demonstrieren, dass der Schutz nicht nur des eigenen Know-hows, sondern auch des Know-hows von Kunden und Lieferanten einen hohen Stellenwert besitzt, wird immer mehr zu einer Selbstverständlichkeit. Dazu gehört nicht nur, dem Kunden zu erklären, dass dieses Thema ernst genommen wird und sich jeder Mitarbeiter dieser Aufgabe verpflichtet hat, sondern auch die explizite Darstellung von Verantwortlichkeit durch die Ausprägung entsprechender Rollen und deren Darstellung im offiziellen Organigramm des Unternehmens.

2.4.1 IT-Security im Organigramm

2

Wird ein Arbeitsplatz »Manager IT-Security« geschaffen, dann stellt sich die Frage, wo im Organigramm diese Aufgabe am besten aufgehängt werden sollte. Hinter dieser Frage stehen neben der Frage nach der höchsten Effizienz auch auszuprägende Prozesse, Rollenbeschreibungen, Verantwortlichkeiten und nicht zuletzt die Ausübung von Macht. Aus diesem Grund sind langwierige Diskussionen rund um dieses Thema üblich.

Ein weiterer Faktor ist die Entwicklung der IT-Security über die letzten Jahre. Eine Vorreiterrolle im Bereich Security hat nachvollziehbar die IT-Abteilung gespielt. In der IT werden die Daten verarbeitet und durch die IT werden die Rechenzentren betrieben. Möchte ein Mitarbeiter Daten austauschen oder möchte er mehr Zugriffsrechte zugewiesen bekommen, dann muss er die IT fragen. Auch wenn es, insbesondere in großen Unternehmen, infolge der Automatisierung solcher Dienstleistungen zunehmend eine wahrnehmbare Trennung von Rechtezuweisungen und IT gibt und auch wenn die IT immer mehr als ein Dienstleister gesehen wird, bleibt auf der anderen Seite im Zuge der neuen Technologien ihr Einfluss mindestens bestehen oder wird sogar noch größer. In der Folge berichtet auch heute noch die überwiegende Anzahl an Managern IT-Security direkt an den IT-Leiter. Das hat vor allem in kleinen und mittelständischen Unternehmen den Vorteil, dass sich dadurch IT-Fachwissen und die Aufgabe des Informationsschutzes synergieträchtig miteinander verbinden lassen. Der Manager IT-Security hat dann neben der rein überwachenden und steuernden Funktion oft auch die Aufsicht oder sogar die administrative Aufgabe, sicherheitsrelevante IT-Systeme zu betreuen oder zumindest über deren Betrieb mitzubestimmen. Je näher er also an der Basis



(in diesem Fall der IT) sitzt, desto fachbezogener wird er agieren können. Dazu kommen technische Entscheidungen bei Notfällen und detaillierte Festlegungen im Rahmen der Erstellung von Richtlinien. Weichen diese von der gelebten Wirklichkeit allzu sehr ab, so wird es schwierig sein, diese in den Betrieb zu überführen. Alles Argumente, den Manager IT-Security in der IT oder nahe an der IT einzusetzen.

Neben diesen offensichtlichen Vorteilen birgt diese Konstellation auch Nachteile, die immer etwas mit Interessenkonflikten, eingeschränkter Awareness bei der Unternehmensleitung und mangelnden Weisungsbefugnissen zu tun haben.

Die IT-Security als natürliches Anhängsel der IT zu sehen, ist deshalb nicht angebracht, es sollten vielmehr alle Alternativen diskutiert werden, und dazu gehören die Anbindung

- an die Unternehmensleitung,
- den Vorstand,
- den Leiter der Personalabteilung,
- an den CIO, also an den Leiter der IT, oder
- an den Datenschutzberechtigten.

Daneben gibt es noch eine weitere, eher seltenere genutzte Möglichkeit, nach der der Manager IT-Security innerhalb der internen Revision oder der Rechtsabteilung angesiedelt ist.

Tipp

Je größer ein Unternehmen ist, desto mehr Spielraum wird vorhanden sein, die Funktion IT-Security möglichst optimal – sprich unabhängig – auszurichten und dementsprechend in die Organisationsstruktur einzubinden.

Die Frage der Zuordnung dieser Funktion wird im Spannungsdreieck zwischen den Grundanforderungen »Gewaltenteilung«, »Befugnisse« und »Effizienz« widergespiegelt.



KAPITEL 2 – ORGANISATION DER IT-SECURITY



Abbildung 2.2: Der Manager IT-Security im Spannungsfeld der Interessen

Dafür steht das Prinzip der Gewaltenteilung: Derjenige, der Richtlinien aufstellt und überprüft, sollte nicht auch derjenige sein, der diese nachfolgend technisch umsetzt bzw. täglich damit konfrontiert wird. Dieser Interessenskonflikt schwächt die Stellung des Managers IT-Security und führt häufig zu schwachen Regeln oder einer mangelhaften Umsetzung.

Ein letzter Punkt betrifft die Befugnisse. Ein Manager IT-Security, der in der IT angesiedelt ist, wird immer einem CIO, also dem IT-Leiter, unterstellt sein. Priorisiert dieser die IT-Security nicht in erforderlichem Maße, so werden unangenehme Regelungen schwer bis überhaupt nicht durchsetzbar sein.

Die letzten beiden Punkte sprechen für eine Ansiedlung außerhalb der IT mit direkter Berichtslinie zur Unternehmensleitung oder zum Vorstand.

Das Fazit, das die verschiedenen Standards und Best-Practice-Ansätze letztlich daraus folgern, ist, dass es in den meisten Fällen nicht ratsam ist, die IT-Security-Organisation mit ihren weitreichenden Aufgaben und einem Wirkungsbereich, der das gesamte Unternehmen berührt, einer IT-Abteilung zu unterstellen. Dieser Ratschlag bezieht sich im Allgemeinen auf größere Unternehmen oder aber auf Unternehmen, die aufgrund rechtlicher Vorgaben, z.B. nach dem IT-Sicherheitsgesetz, ein stark ausgeprägtes IT-Security-Umfeld aufbauen müssen. Die Gründe sind indes die gleichen: Die Durchset-



zung von Sicherheitsmaßnahmen mit der erforderlichen Konsequenz ist in einer zu IT-nahen Konstellation nur schwer vorstellbar. Dies liegt in der Natur von Sicherheitsmaßnahmen, da diese, als Art Versicherung, häufig auf eventuell in der Zukunft eintretende Ereignisse reagieren und damit oft nicht die gleiche Priorität haben wie der Betrieb der IT-Systeme. Grundsätzlich ist also zu empfehlen, die IT-Security-Organisation so einzuordnen, dass ein direkter Berichtsweg zu den obersten Leitungsinstanzen besteht und dass der Manager IT-Security im Auftrag dieser Instanzen agiert.

In kleinen Unternehmen

Die Frage der Organisation von IT-Security wird umso stärker diskutiert, je größer ein Unternehmen wird. In einer typischen kleineren mittelständischen Firma wird der Manager IT-Security vermutlich in der IT-Abteilung sitzen und den Job zu x % ausfüllen. Daneben wird er Administrator sein, das Netzwerk betreiben, Software entwickeln oder eine andere IT-Funktion wahrnehmen.

In diesen Unternehmen hat sich die Aufgabe, sich auch um die IT-Security zu kümmern, häufig aus der IT-Abteilung heraus entwickelt, und auch heute noch steht und fällt der Einfluss des IT-Security-Experten mit der Unterstützung durch den IT-Leiter. Die eigentlich sinnvolle Gewaltentrennung zwischen dem Ersteller von Richtlinien und der IT, die diese umsetzen soll, wird nicht wahrgenommen. Dieser Nachteil kann aber wiederum durch größere Flexibilität und höhere Praxisnähe ausgeglichen werden.

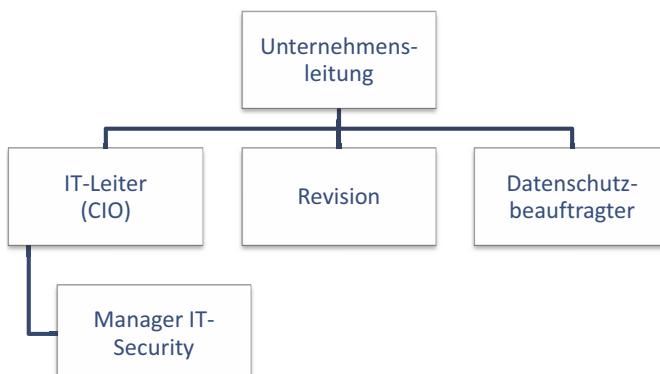


Abbildung 2.3: IT-Security innerhalb der IT



KAPITEL 2 – ORGANISATION DER IT-SECURITY

Die Durchsetzbarkeit von Richtlinien und Maßnahmen gegenüber den Fachabteilungen ist ganz besonders in dieser Konstellation nicht nur von der IT-Leitung, sondern im besonderen Maße von der Unternehmensleitung abhängig. Fehlt das klare Bekenntnis mit Wort und Tat zu den Zielen der IT-Security im Allgemeinen und den Kompetenzen des Managers IT-Security im Besonderen, dann wird die Umsetzung eines akzeptablen Sicherheitsniveaus schwer bis unmöglich sein.

In großen Unternehmen

Die Gewaltenteilung zwischen der Führungsaufgabe des Managers IT-Security und dem IT-Betrieb bedingt eine Trennung von IT und IT-Security. In diesem Fall wird der Manager IT-Security direkt der Unternehmensleitung unterstellt und kann dadurch auf Augenhöhe mit dem Leiter der IT zusammenarbeiten. Eine Zuordnung der IT-Security zum Vorstand stellt eine weitere Möglichkeit dar, die funktionale Trennung zu unterstreichen.



Abbildung 2.4: IT-Security direkt der Unternehmensleitung unterstellt

In einer häufig anzutreffenden Konstellation werden alle Sicherheitsbereiche unter einem Koordinator zusammengefasst. Dieser verantwortet neben der IT-Security auch den Datenschutz, häufig in der Rolle des Datenschutzbeauftragten, den Arbeitsschutz und die Gebäudesicherheit sowie weitere Bereiche, falls sie in diese Funktionen hineinspielen. Der Manager IT-Security wird in diesem Fall die IT im Fokus haben und damit sowohl die Interessen der IT-Security vertreten als auch zusammen mit den anderen Sicherheitsbereichen gemeinsam Lösungen für deren Aufgabenstellungen umsetzen. Diese Organisationsform erleichtert z.B. die Umsetzung von baulichen Maßnahmen aus Sicht der IT-Security und die Wahrnehmung der laufenden Aufgaben der Gebäudesicherung, z.B. Kontrollgänge durch den Werkschutz.



VERANKERUNG IM UNTERNEHMEN

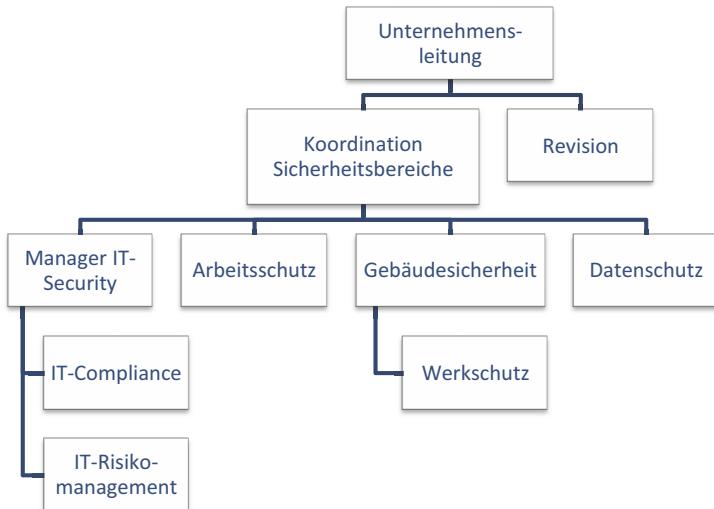


Abbildung 2.5: Einführung einer Koordinationsstelle für alle Sicherheitsbereiche

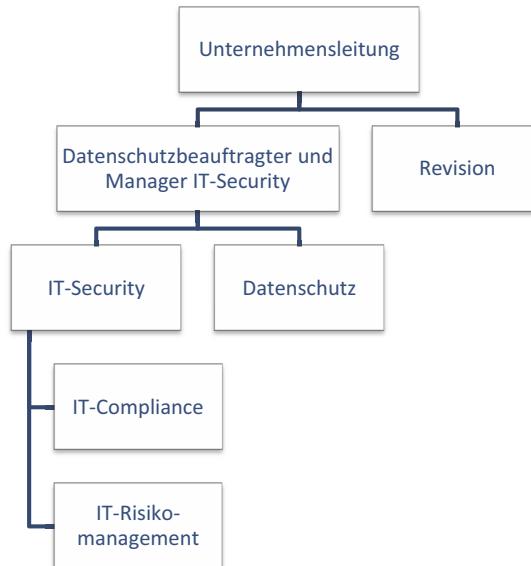
2

Eine weitere Aufgabe des Managers IT-Security innerhalb einer solchen Konstellation wird die Kommunikation in Richtung der IT sein.

Zusammenlegung IT-Security und Datenschutz

Die strikte Trennung zwischen der IT-Security und der Aufgabe des Datenschutzes, wie sie vor einigen Jahren noch verfolgt wurde, wird heute nicht mehr vollzogen. Ganz im Gegenteil geht der Trend eher dahin, den Bereich IT-Security dem Datenschutzbeauftragten unterzuordnen oder zumindest beide Bereiche eng miteinander zu koppeln.

Der Grund für diese Vorgehensweise liegt vor allem darin begründet, dass der technische Datenschutz die gleichen Ziele verfolgt wie die IT-Security. Außerdem wurde bald erkannt, dass eine Trennung von Daten mit personenbezogenem Hintergrund und anderen Daten wie z.B. Zeichnungsdaten kaum stringent durchzuhalten ist und es daher logisch erscheint, einfach anzunehmen, dass alle Daten auch einen datenschutzrelevanten Hintergrund haben könnten.



2

Abbildung 2.6: IT-Security und Datenschutz innerhalb einer Organisationseinheit

Lokale IT-Security-Manager

Unternehmen mit vielen Außenstellen werden sich immer vor die Frage gestellt sehen, ob eine zentrale Stelle für die IT-Security ausreichend ist oder ob gewisse Tätigkeiten nicht dezentral vor Ort durchgeführt werden müssen. Dies hat dazu geführt, dass es heute weitgehend üblich ist, dem global zuständigen Manager IT-Security in Außenstellen einen Mitarbeiter zuzuordnen, der lokal für die Belange der Sicherheit zuständig ist. Je nach Größe des Unternehmens und der Größe der Außenstelle wird dies häufig nur eine Zuordnung zu einem bestimmten Prozentsatz sein, gewährleistet aber eine höhere Transparenz und eine effektivere Durchschlagskraft im Rahmen der Umsetzung von Maßnahmen und des Tagesgeschäfts. Der Mitarbeiter berichtet dabei fachlich an den Manager IT-Security und wird von diesem im Gegenzug in eine regelmäßige Kommunikation eingebunden.

Typische Aufgaben eines lokal agierenden IT-Security-Mitarbeiters:

- Lokale Umsetzung von zentral festgelegten Richtlinien
- Umsetzung von allgemeinen oder für die Außenstelle definierten Maßnahmen



- Betrieb der lokalen IT-Security-Infrastruktur (Firewalls, Antivirus, Patchmanagement, Betriebssystemsicherheit, Softwaresicherheit)
- Durchführung von Awareness-Maßnahmen in der Außenstelle
- Ansprechpartner für alle lokalen Themen der IT-Security
- Berichtet an den zentralen Manager IT-Security
- Durchführung von Audits

Ein zentral sitzender Manager IT-Security wird, ansteigend mit der Anzahl an Außenstellen, abhängig sein von der Mitarbeit lokal sitzender Mitarbeiter. Das betrifft nicht nur den Betrieb, sondern vor allem auch die Kontrolle von Richtlinien und Maßnahmen. Nur dadurch wird die regelmäßige Überprüfung im Rahmen des kontinuierlichen Verbesserungsprozesses überhaupt möglich sein. Es ist daher zu empfehlen, diese Mitarbeiter eng einzubinden.

Zu beachten ist, dass je nach Kulturreis auch die Vorgehensweise bei der Umsetzung von Maßnahmen und der Betrieb von IT-Security an die lokalen Gegebenheiten und ebenso kulturellen Gepflogenheiten anzupassen ist. Dies muss allerdings geschehen, ohne das geforderte Sicherheitsniveau zu unterschreiten.

2.4.2 IT-Security und der Datenschutz

Der technische und organisatorische Datenschutz spielt für den Datenschutzbeauftragten eine große Rolle. Er delegiert diese Pflicht im Normalfall an die verarbeitende Stelle. Zumindest in der IT wird dies häufig der IT-Leiter sein. Dieser hat dann auf die Umsetzung von technischen Maßnahmen zum Schutz personenbezogener Daten nach dem Stand der Technik hinzuwirken. Diese Maßnahmen wiederum zielen in den Verantwortungsbereich des Managers IT-Security, und damit ist die Rollenverteilung festgelegt: Der Datenschutzbeauftragte definiert, welche Daten zu schützen sind. Der Datenschutz spricht in diesem Fall nicht von Daten oder Applikationen, sondern von Datenverarbeitungen. Die IT-Abteilung verknüpft diese definierten Verarbeitungen mit den entsprechenden IT-Systemen und Applikationen. Der Manager IT-Security legt die Regeln fest, was erforderlich ist, um das geforderte Schutzniveau zu erreichen, und die IT-Abteilung führt die entsprechenden Maßnahmen durch.



Nach der EU-Datenschutz-Grundverordnung zu schützende Daten, also personenbezogene, elektronisch vorliegende Informationen, werden vom Verantwortlichen für Datenschutz geschützt, indem er Maßnahmen einfordert, die der Manager IT-Security koordiniert und die IT-Abteilung umsetzt. Da personenbezogene und nicht personenbezogene Daten in der Betriebswirklichkeit schwer zu trennen sind, werden die meisten Maßnahmen beide Arten von Daten beeinflussen. Der engen Zusammenarbeit von Datenschutz und Informationsschutz, auf Englisch »data privacy« und »information security«, kommt im Rahmen der IT-Security-Organisation also eine herausragende Stellung zu.

2.4.3 Zusammenspiel mit anderen Sicherheitsbereichen

2

Unternehmenssicherheit

Die Unternehmenssicherheit hat ihren Fokus auf Themen, die als Sicherheitsthemen bezeichnet werden, die aber weniger mit dem Betrieb von IT-Systemen zu tun haben. Dazu gehören klassisch Felder wie das Krisenmanagement, der Schutz von Personen auf Dienstreisen und Veranstaltungen oder auch die Zusammenarbeit mit Sicherheitsbehörden. In vielen Fällen stellt die Unternehmenssicherheit damit eine der IT-Security übergeordnete Instanz dar. Eine Aufgabe, die als Beispiel dafür dienen kann, ist das Krisenmanagement. Installiert ein Angreifer eine Erpressersoftware auf einer Produktionsmaschine, deren Ausfall große Kosten verursachen würde, dann wäre dies ein Fall, den zuallererst die Unternehmenssicherheit aufnehmen würde. Sie würde natürlich auch die IT-Security hinzuziehen, daneben aber noch die Behörden informieren, mit den Produktionsverantwortlichen sprechen, einen Krisenstab einrichten, entscheiden, ob auf den Erpressungsversuch geantwortet werden soll, und letzten Endes mit der Kommunikationsabteilung über das Für und Wider einer Veröffentlichung des Vorfalls diskutieren.

Neben diesem Beispiel kann es viele weitere Regelungen geben, die in Zusammenarbeit der Unternehmenssicherheit und der IT-Security erarbeitet werden müssen. So kann es Aufgabe der Unternehmenssicherheit sein, die Länge für Passwörter der Benutzer festzulegen, da dies eine Vorgabe ist, die alle Mitarbeiter betrifft. Die IT-Security wiederum kann verantwortlich für die Passwörter der IT-Administratoren sein.



Diese Beispiele zeigen, dass es zum einen sehr wichtig ist, die Aufgabenfelder genau zu definieren und dies auch zu dokumentieren, zum anderen aber auch die Tatsache, dass es für eine solche Regelung keine Blaupause geben kann. Eine solche Regelung wird individuell in jedem Unternehmen einzeln festgelegt werden müssen.

Werkschutz

Der Werkschutz kümmert sich um den Schutz physischer Werte durch Maßnahmen wie die Zutrittskontrolle oder die Überwachung von Gebäuden durch Kontrollgänge. Nicht autorisierter Zutritt zu sensiblen Bereichen, insbesondere zu Zeiten, in denen kein anderer Mitarbeiter anwesend ist, kann nur durch den Werkschutz bemerkt und gemeldet werden. Neben der reinen Kontrolle und Überwachung ist damit auch die Alarmierung eine grundlegende Aufgabe des Werkschutzes.

Im IT-Security-Management-Bereich Business Continuity Management, insbesondere in der Bearbeitung von Notfällen, kommt dem Werkschutz damit die Aufgabe zu, im Falle von physischen Sicherheitsereignissen die Erstalarmierung vorzunehmen. So müssen entsprechende Alarmierungsvorschriften und Alarmierungslisten abgestimmt sein, die z.B. bei Feuer oder Wassereinbruch abgearbeitet werden können. In diesem Fall arbeitet der Werkschutz zum einen dem Verantwortlichen für die Unternehmenssicherheit und dem Manager IT-Security und anderen internen Sicherheitsbereichen zu, auf der anderen Seite muss die Zusammenarbeit mit öffentlichen Organen wie der Polizei oder der Feuerwehr reibungslos funktionieren.

Protokolle über Kontrollgänge oder die Sichtung verdächtiger Personen sind eine wichtige Grundlage für die Durchführung von forensischen Maßnahmen bei einem eingetretenen Datendiebstahl und müssen deshalb auch für einen längeren Zeitraum archiviert werden.

Der Werkschutz hat außerdem die Aufgabe, sicherzustellen, dass sich nur Personen mit Zugangsberechtigung in sensiblen Bereichen aufhalten. Besucher werden häufig zudem begleitet, bis ein Mitarbeiter aus dem Fachbereich diese Aufgabe übernimmt. So soll verhindert werden, dass sich Fremde einschließen lassen oder frei herumlaufen und Einsicht in sensible Daten nehmen können. In diesem Zusammenhang ist die Ausstellung von Besucherausweisen Teil der Identifizierung und Zutrittsdokumentierung von Besuchern.



Gebäudemanagement

Die Mitarbeiter des Bereichs Gebäudemanagement oder Facility-Management tragen dafür Sorge, dass die grundlegenden Installationen vorhanden sind, die zur Nutzung eines Gebäudes erforderlich sind. Bezogen auf das IT-Security-Management handelt es sich dabei vor allem um Einrichtungen zur Zutrittskontrolle, die Zufahrtskontrolle, Brandschutzmaßnahmen, Überwachungseinrichtungen, Einbruchsschutz und bauliche Maßnahmen zur Abschottung sensibler Bereiche wie z.B. des Rechenzentrums.

Das Gebäudemanagement trägt also Sorge dafür, dass in Abstimmung mit dem Werkschutz und dem Manager IT-Security Überwachungskameras in einer Art und Weise installiert werden, dass sowohl die Belange der IT-Security als auch des Datenschutzes sichergestellt sind. In dieser Funktion stellt es die Infrastruktur zur Verfügung, auf die das IT-Security-Management aufsetzt. Werden hier Fehler begangen oder wichtige Punkte außer Acht gelassen, so ist dies später kaum wieder durch organisatorische Maßnahmen aufzufangen.

2

Arbeitssicherheit

Der Sicherheitsingenieur trägt dafür Sorge, dass die körperliche Unversehrtheit der Mitarbeiter gewährleistet ist. Damit greift er in Arbeitsvorgänge, die Maschinensteuerung, die Verlegung von Kabeln und bauliche Maßnahmen ein. Der Arbeitsschutz basiert auf dem Arbeitsschutzgesetz und hat damit im Gegensatz zu den anderen Sicherheitsbereichen eine definierte gesetzliche Grundlage.

Aus der Historie waren die Sicherheitsingenieure oft die Ersten, die sich auch mit der Datensicherheit auseinandergesetzt haben. In einigen Firmen sieht man deshalb Organigramme, in denen der IT-Security-Experte an den Verantwortlichen für Arbeitssicherheit berichtet.

Interne Revision

Die interne Revision nimmt innerhalb eines Unternehmens eine Kontrollfunktion wahr. Sie berichtet an die Unternehmensleitung oder den Aufsichtsrat und hat somit die Aufgabe, regelmäßige Audits durchzuführen und deren Ergebnisse auszuwerten und zu präsentieren. Neben Feldern wie den Finanzen, Kreditrisiken oder operativen Risiken werden auch IT-Systeme, IT-Pro-



zesse und Applikationen geprüft. Auf diesen letzten Feldern überlappen sich also die Prüfungen von Revision und IT-Security. Geht es um Applikationssicherheit eines Produktions- oder Abrechnungssystems, so ist die Sicherstellung von Vertraulichkeit, Verfügbarkeit und Integrität für beide Organisationsbereiche interessant.

Der Unterschied liegt also weniger an den Themen, sondern eher in der Tiefe, in der eine Überprüfung stattfindet. Bezogen auf das Produktionssystem wird die Revision eher auf das darunterliegende Rollensystem und die Zugriffsbe rechtigungen abheben, während die IT-Security daneben noch die Systemsi cherheit des Rechners prüfen sollte, auf dem die Software installiert ist. Arbeiten beide Bereiche zusammen, so lassen sich einige Synergieeffekte erzielen. Dazu kommt, dass insgesamt in erheblich größerem Umfang geprüft werden kann, wenn eine gewisse Arbeitsteilung stattfindet.

2

Wichtig

Im Gegensatz zu einem Mitarbeiter aus der Revisionsabteilung hat der Manager IT-Security zusätzlich eine beratende Funktion. Werden Schwachstellen aufgedeckt, so wird er in der Lage und auch in der Pflicht sein, diese Schwachstelle zu bewerten und angemessene Maßnahmen vorzuschlagen.

Eine weitere weitverbreitete Tatsache ist, dass die interne Revision traditions gemäß einen höheren Stellenwert innerhalb eines Unternehmens innehat als die IT-Security. Mit dem Vehikel Revision lassen sich also unter Umständen auch langfristige und kostenintensive Maßnahmen einführen und mit der nötigen Durchschlagskraft verfolgen.

IT-Administrator

Der IT-Administrator ist immer auch ein IT-Security-Experte. Diese Aussage soll plakativ darstellen, wie wichtig es ist, dass ein IT-Administrator bei allen seinen Handlungen immer auch die Sicherstellung von Vertraulichkeit, Verfügbarkeit und Integrität von Daten im Auge hat. Da es nahezu unmöglich ist, für alle Verfahren und alle Installationen entsprechende Richtlinien zu verfassen, ist es unabdingbar, dass ein Administrator seine Handlungen hinter fragt, bevor er mit diesen beginnt.



KAPITEL 2 – ORGANISATION DER IT-SECURITY

IT-Administratoren konfigurieren, pflegen, überwachen und betreiben IT-Systeme, Netzwerke und Applikationen und damit nahezu alle Systeme, die Daten verarbeiten. Treten Sicherheitsprobleme auf, so wird der Administrator der Erste sein, der diese bemerkt, und der Erste, der sie beheben kann. Er ist das Bindeglied zwischen den Daten und dem IT-Security-Management, ohne das ein IT-Security Lifecycle nicht möglich ist.

Ein verantwortlich handelnder Administrator wird seine Bedenken offen kommunizieren, auch wenn dies weitere Aufwände zur Folge haben könnte. Als Experte wird ihm zudem die Aufgabe zukommen, Maßnahmen zu implementieren und deren Umsetzung und Betrieb zu bewerten. Dasselbe gilt für Richtlinien, deren Alltagstauglichkeit nur durch einen Administrator, der mit den betroffenen Systemen befasst ist, sichergestellt werden kann.



3 IT-Compliance

3.1 Kapitelzusammenfassung

Die IT-Compliance gibt vor, welche Tätigkeiten innerhalb der IT-Abteilung aufgrund gesetzlicher, normativer oder interner Vorschriften und Vorgaben durchzuführen sind. Das können z.B. Vorgaben zur Vorratsdatenspeicherung sein oder Vorschriften über die sichere, elektronische Ablage von Buchungsbelegen. In diesen Fällen zielt das entsprechende Gesetz nicht direkt auf die IT, sondern spricht das Unternehmen an, in letzter Instanz aber ist es auf technische Art und Weise zu realisieren.

Hinweis

Auch wenn es keine gesetzliche Grundlage gibt, die den Aufbau einer IT-Security-Organisation explizit fordert, so ist dies z.B. in Verträgen mit Kunden oft direkt vereinbart. Der Kunde möchte darauf Einfluss nehmen können, wie seine eigenen Daten verarbeitet werden, und sieht die Kontaktstelle beim Lieferanten oder Auftragnehmer in dieser Organisationseinheit.

In Bezug auf das Thema IT-Security verhält es sich ähnlich. Es gibt kein Gesetz, das den Aufbau und den Betrieb einer IT-Security-Organisation explizit vorschreibt, aber es ergibt sich automatisch, wenn man die entsprechenden Vorgaben sinnvoll umsetzen möchte. Ein Beispiel hierfür ist die EU-DSGVO. Viele darin enthaltene Vorgaben zielen zunächst einmal auf das Unternehmen und die Unternehmensleitung, diese wird die darin beschriebenen Aufgaben, wie die Planung und Umsetzung von Technisch-Organisatorischen Maßnahmen (TOM), aber direkt der IT zuordnen, die dann, zusammen mit der IT-Security, entsprechende Maßnahmen entwickeln und umsetzen muss. So müssen personenbezogene Daten klassifiziert und aufgrund ihrer Klassifizierung geschützt werden. Die dabei zum Tragen kommenden Schutzziele entsprechen den klassischen Schutzzielen der IT-Security: Vertraulichkeit, Ver-



KAPITEL 3 – IT-COMPLIANCE

fügbarkeit und Integrität. Hinzu kommt noch die »Belastbarkeit«. An dieser Stelle nun werden der Datenschutz, die IT und die IT-Security zusammengeführt. Der Datenschutzbeauftragte gibt die Richtung vor, die IT erfasst die auf ihren technischen Systemen durchgeführten Verarbeitungen, verknüpft diese mit den entsprechenden Daten und Systemen und beachtet, wenn es um den Schutz dieser Daten geht, die Maßnahmen, die die IT-Security per Richtlinien vorgibt. Es würde also wenig Sinn machen, wenn die IT-Security Richtlinien nur für datenschutzrelevante Daten erstellt und parallel dazu weitere für nicht-personenbezogene Daten.

3

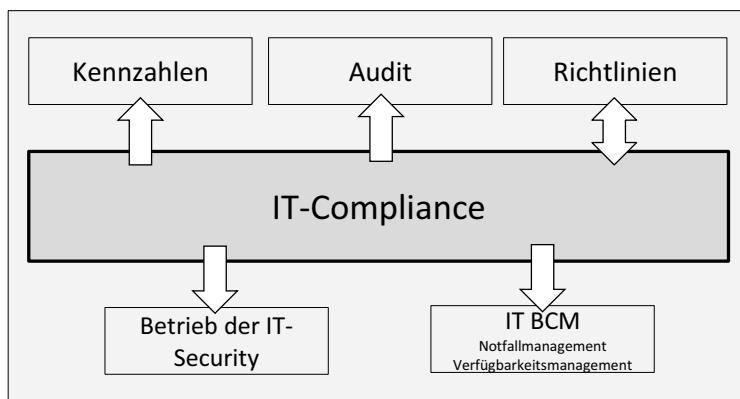


Abbildung 3.1: Primäre Abhängigkeiten von anderen Themen der IT-Security

Der Manager IT-Security wird damit zu einem wichtigen Prozess-Eigentümer, wenn es um die Umsetzung von Compliance geht. Er wirkt maßgeblich bei der Definition von Vorgaben mit, erlässt Regeln und prüft diese auch. Ein tiefes Verständnis für die zugrunde liegenden Vorschriften ist daher unerlässlich.

In weltweit tätigen Unternehmen gehört es dazu, auch die wesentlichen Gesetzgebungen derjenigen Länder zu kennen, in denen das eigene Unternehmen entweder Tochterunternehmen betreibt oder in denen Kunden beheimatet sind. Um den Überblick zu behalten, empfiehlt es sich daher, Dienstleistungen wie sogenannte »Law Tracker« in Anspruch zu nehmen. Dabei handelt es sich zumeist um Applikationen in der Cloud, die eine Übersicht relevanter Gesetze bereits aufbereitet darstellt und auch Vergleiche zwischen den Gesetzgebungen anstellen kann. Wenn man z.B. ein Tochterunternehmen in Südafrika hat und Details über die lokale Gesetzgebung in Bezug



auf personenbezogene Daten wissen möchte, dann kann man eine solche Dienstleistung nutzen.

Zur besseren Übersicht kann man die jeweils wichtigen Gesetze einer Jurisdiktion in einem »Compliance Register« auflisten und entsprechende, getroffene Maßnahmen mit den jeweiligen gesetzlichen Vorgaben verknüpfen. Auf diese Art und Weise ist es später leichter, den Nachweis zu führen, dass lokales Recht adäquat umgesetzt wurde.

Die Top-4-Fragen zum aktuellen Kapitel:

- Liegt der Ausrichtung des IT-Security-Managements eine interne oder externe Vorgabe oder eine Norm zugrunde?
- Sind die internen und externen Vorgaben, die für das IT-Security-Management von Relevanz sind, identifiziert worden?
- Ist die Zusammenarbeit des Managers IT-Security mit dem Datenschutzbeauftragten abgestimmt?
- Ist geregelt, wie der Manager IT-Security in die Unternehmens-Compliance eingebunden ist?

3

3.2 Einführung

Der Begriff Compliance geistert seit Jahren durch zahllose Präsentationen zum Thema IT und IT-Security. Bei genauerem Nachfragen offenbaren sich allerdings regelmäßig Missverständnisse, die darauf beruhen, dass er durchaus unterschiedlich interpretiert werden kann. Formal bedeutet das Wort »Compliance« das regelkonforme Verhalten eines Unternehmens (oder auch einzelner Mitarbeiter) in Bezug auf gesetzliche, regulative, externe und eigene Regelungen. Die Frage lautet demnach: »Compliance in Bezug auf was?« Aus welchem Blickwinkel und mit welcher Gewichtung man die unterschiedlichen Vorgaben betrachtet, hängt stark vom Betrachter ab. Daraus folgt, dass es so gut wie keine externe Regelung gibt, die in einem multinationalen Unternehmen an jedem Standort in jedem Land auf exakt die gleiche Weise umzusetzen wäre. Die jeweils unterschiedlich ausgeprägte, nationale Gesetzgebung wirkt sich genauso aus wie die unterschiedlichen Vorgaben von Kunden oder Verbänden. Schreibt ein Kunde zur Datenübermittlung bestimmte Verschlüsselungsalgorithmen vor, dann kann es leicht passieren, dass diese in einem anderen Land der Erde von staatlicher Seite aus untersagt sind.



KAPITEL 3 – IT-COMPLIANCE

Gelten diese Grundannahmen schon für ein einzelnes Unternehmen, dann wird schnell deutlich, dass es auch keine allgemeingültige Antwort darauf geben kann, welchen Regelungen jedes beliebige Unternehmen grundsätzlich zu folgen hat. Neben den nationalen Gesetzen, die vom Standort abhängig sind, hängen viele weitere Vorgaben von Parametern wie der Branche oder den Kunden ab. Man denke nur an die unterschiedlichen Vorgaben von Restaurantketten im Gegensatz zu Unternehmen, die Rüstungsgüter produzieren.

Möchte man nun eine Handlung von den existierenden Compliance-Vorschriften ableiten, so ist zu beachten, dass die unterschiedlichen Vorgaben nicht auf einer Ebene agieren, sondern wie ein Filtersystem mit verschiedenen Filtergrößen wirken. So haben Gesetze und Betriebsvereinbarungen Vorrang vor internen Richtlinien. Vereinbarungen mit Kunden und Lieferanten wiederum werden sich zunächst auch an Gesetzen ausrichten müssen. Das hilft aber nur in den Fällen weiter, in denen die Rechtslage so formuliert wurde, dass sich daraus wirkliche Handlungsgrundsätze ableiten lassen, und das ist deutlich seltener der Fall. Das kann auch an der großen Anzahl von sich zum Teil widersprechenden Gerichtsurteilen ermessen werden, die man dem Bereich IT-Security zuordnen kann. Ein gutes Beispiel ist aktuell die EU-Datenschutz-Grundverordnung (EU-DSGVO). Seit dem 25. Mai 2018 muss diese in allen Unternehmen umgesetzt sein, die mit personenbezogenen Daten europäischer Bürger arbeiten. Wenn man aber nun ins Detail geht, dann wirft dieses Gesetz eine Menge Fragen auf. Das beginnt schon bei so wichtigen Punkten wie den Schutzz Zielen. Sind die Schutzz Zielen Vertraulichkeit, Verfügbarkeit und Integrität bereits seit Jahren bekannt, so stellt sich die Frage, welche Bedeutung dem neu hinzugefügten Schutzz Ziel »Belastbarkeit« zukommt. Andere zentrale Themen wie »privacy by default« oder »privacy by design« werfen ähnliche Fragen auf. Auch diese werden in den kommenden Jahren beantwortet werden müssen, bevor Unternehmen diese Vorgaben rechtssicher umsetzen können.

Bevor die EU-DSGVO aufgrund der hohen potenziellen Bußgelder den Schutz von personenbezogenen Daten massiv in den Vordergrund gerückt hat, gab es vor allem zwei gesetzliche Grundlagen, die den verantwortlichen Umgang mit eigenem und fremdem Know-how betont haben und die aus diesem Grund, zumindest in Deutschland, auch häufig zitiert werden. Dabei handelt es sich um die beiden folgenden Gesetzesvorschriften:

**■ GmbH-Gesetz § 43 Abs. 1 und 2**

- (1) Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden.
- (2) Geschäftsführer, welche ihre Obliegenheiten verletzen, haften der Gesellschaft solidarisch für den entstandenen Schaden.

■ Aktiengesetz § 91 Abs. 2

- Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.

Beide aufgeführten Gesetze zeigen explizit die Verantwortung der Unternehmensleitung für das Know-how als Basis für die Sicherstellung des Betriebs des Unternehmens.

3

Wichtig

Der Datenschutzbeauftragte hat die Hinwirkungspflicht zur Umsetzung von IT-Security-Maßnahmen, um personenbezogene Daten zu schützen. Der Manager IT-Security hat die Aufgabe, die technische Umsetzung zu steuern.

Die IT-Compliance ist als Teil der Unternehmens-Compliance zu sehen. Diese wiederum bestimmt zu einem guten Teil die Ausgestaltung der Governance im Unternehmen. Die Compliance definiert damit, was zu tun ist und mit welcher Priorität, diese kann z.B. auf Basis der zu erwartenden Strafen und Beeinträchtigungen definiert werden, und die Governance beantwortet die Frage, welche Organisationseinheit diese Anforderungen umzusetzen hat. Teilaspekte sind dabei die erforderlichen Kompetenzen und Ressourcen. Da ähnliche Unternehmen, die ähnlich aufgestellt sind, auch vergleichbare Anforderungen an diese Umsetzungen haben, macht es Sinn, hier Standards und Best-Practice-Ansätze zu folgen. Die entsprechenden Branchenstandards wiederum werden so generisch aufgebaut, dass sie einfach und umfassend verwertbar sind. Standards und Normen gewinnen damit stark an Bedeutung. Denn dort, wo der exakte Rahmen fehlt, setzen sie die Maßstäbe und gewährleisten, dass die eigene Vorgehensweise zeitgemäß und mit der anderer Unternehmen vergleichbar ist.



KAPITEL 3 – IT-COMPLIANCE

Im Informationsschutz sind seit Mitte der 1990er Jahre etliche Normen und Best-Practice-Kataloge im Umlauf. Viele davon finden heute Anwendung in mittleren und großen Unternehmen. Dazu gehören z.B. ITIL, COBIT, die Schriften des Bundesamts für Sicherheit in der Informationstechnik (BSI) oder die ISO-27000-Reihe. Dazu kommen einige gesetzliche Vorschriften wie die des Telekommunikationsgesetzes (TKG), der EU-Datenschutz-Grundverordnung (EU-DSGVO) oder des Sarbanes-Oxley Acts.

Schaut man sich auf dem Markt um, dann findet man zudem eine unübersichtlich große Anzahl von Dienstleistern, die jeweils einen dieser eben beschriebenen Teilbereiche, zumeist aus technischer Sicht, bedienen. Vertreten sind unter anderem Produkte, die

- Rechtestrukturen auf Servern überprüfen und auf Übereinstimmung (ein anderes Wort für Compliance) mit den Richtlinien für die Zugriffskontrolle abprüfen,
- aktive Netzwerkkomponenten abfragen und deren Konfiguration auf Unstimmigkeiten abprüfen,
- Umsetzung von Rollenkonzepten auf Software-Plattformen überprüfen und unzulässige Rollenüberschneidungen aufzeigen,
- vorhandene Softwarelizenzen gegen den Ist-Bestand an Software prüfen, um die Produkte zu ermitteln, die nachlizenziert werden müssen, oder
- Wartungsverträge durchleuchten, um Verbesserungspotenziale zu entdecken.

Diese Produkte hängen sich an den Begriff IT-Compliance, decken auch die eine oder andere Vorgabe ab, können aber keinen umfassenden Schutz bieten. Dazu kommt, dass sich einige dieser Produkte von der Kernaufgabe des Informationsschutzes immer weiter entfernen. So ist das Lizenzmanagement zwar eine Aufgabe der Compliance, hat aber mit IT-Security nicht viel zu tun. Damit spielen diese Produkte auch in der Implementierung und dem Betrieb eines IT-Security-Managements allenfalls die Rolle unterstützender Tools.

Der Fokus technischer Produkte liegt vornehmlich darin, Schwachstellen aufzudecken und Missbrauch zu verhindern. Ihre Daseinsberechtigung haben sie vor allem deswegen, weil sie jeweils ein Gebiet bearbeiten, in dem die Konzentration an sensiblen und kritischen Daten hoch ist und es dementsprechend wichtig ist, an diesen Stellen für Sicherheit zu sorgen. So ist es auch für



Firmen, die sich gegen die Implementierung eines IT-Security-Managements aussprechen, wichtig, für Zugriffsregeln auf Datenservern, für Notfallpläne oder die Netzwerksicherheit zu sorgen. Dabei handelt es sich um Maßnahmen, deren Erforderlichkeit aus den oben genannten Gesetzen abgeleitet werden kann.

Wichtig

Es gibt nicht das Gesetz oder die Sammlung an Gesetzen, die der Manager IT-Security in die Hand nehmen kann, um den Umsetzungsgrad an Unternehmens-Compliance zu überprüfen. Er muss sich mit den verschiedenen Gesetzen auseinandersetzen, die je nach eingesetzter Infrastruktur, Rechtsform des Unternehmens und Standort verschieden sein können. Diese Gesetze dienen aber nur als Ausgangspunkt, um den Rahmen, in dem sich die Datenverarbeitung bewegen darf, zu definieren. Die genaue Ausprägung lässt sich dann im Folgenden auf Basis von Standards und den Vorgaben von Kunden oder Verbänden festlegen.

3

Im Rahmen der Sorgfaltspflicht, zu der alle verantwortlichen Personen verpflichtet sind, müssen Maßnahmen ergriffen werden, um Schaden vom Unternehmen abzuwenden. Zu diesen Maßnahmen gehören auch und vor allem diejenigen, die im Bereich der IT angesiedelt sind. Festgehalten ist dies für Aktiengesellschaften recht unspezifisch im Aktiengesetz unter § 91(2): »Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.« Der Schwerpunkt der Aussage liegt auf dem Begriff »Überwachungssystem« und kann für den Bereich des Informationsschutzes direkt auf ein eingeführtes ISMS bezogen werden.

Im damit vergleichbaren Gesetz, das eine GmbH betrifft (GmbHG), wird kein Überwachungssystem erwähnt, aber in § 43 wird die Sorgfaltspflicht aufgeführt, die ein Geschäftsführer anzuwenden hat. Kommt es zu Auseinandersetzungen, so ist nachzuweisen, dass dieser Sorgfaltspflicht Genüge getan wurde. Ist dies nicht möglich, so greift eine Reihe anderer Gesetze, auf deren Grundlage Strafen verhängt werden können.



3.3 Standards

Aufgrund der fehlenden gesetzlichen Vorgaben, wie genau ein IT-Security-Management umzusetzen ist, kann ein Unternehmen dieses so implementieren, dass die eigenen Belange priorisiert Beachtung finden. Das eröffnet dem Manager IT-Security die Möglichkeit, ein individuell an das Unternehmen angepasstes Sicherheitssystem zu etablieren. Vorhandene Prozesse und Vorgehensmodelle werden dabei idealerweise integriert und weiter ausgebaut.

Hinweis

Die gesetzlich verankerte Forderung nach einem Datenschutzbeauftragten in Unternehmen stellt eine Ausnahme dar, und damit ist das Fehlen der Forderung nach einem Manager IT-Security nicht ungewöhnlich. Gesetze haben nicht die Aufgabe, eine Lösung zu skizzieren, und damit leiten sich viele Anforderungen an Unternehmen in Bezug auf die IT-Security auch nicht direkt aus dem Gesetzestext, sondern aus den entsprechenden Gerichtsurteilen ab.

3

Auf der anderen Seite macht es auch hier keinen Sinn, das Rad erneut zu erfinden, und im Grunde stehen und standen bereits seit Jahren viele Kollegen vor den gleichen Herausforderungen und haben sie bewältigt. Aus diesen Erfahrungen ist eine Reihe von wichtigen Normen entstanden, die heute auf einem Stand sind, der als ausgereift bezeichnet werden kann. International verbreitete Ansätze haben sich dabei weitgehend durchgesetzt, sodass sich auch nationale Empfehlungen wie die des Bundesamts für Sicherheit in der Informationstechnologie (BSI) mehr und mehr daran ausrichten. Unternehmen, die weltweit agieren, haben heute keine andere Möglichkeit mehr, als die Standards umzusetzen, die internationale Anerkennung gefunden haben und deren Umsetzung so etwas wie eine Voraussetzung für Geschäftsanbahnungen geworden sind. Geschäftspartner sprechen heute von den gleichen Prozessen und Grundsätzen, wenn es um das Thema IT-Security geht, und das ist nicht Gesetzen geschuldet, sondern einer Reihe von wichtigen Standards.

In Deutschland haben wir eine spezifische Situation, die andere Länder in dieser Ausprägung nicht kennen. Schon früh hat das BSI sehr detaillierte Anforderungen an die IT-System-Sicherheit gestellt und diese auf Hunderten von Seiten publiziert. Das dabei entwickelte Wissen kann, soweit es die IT-



Grundschutz-Kataloge betrifft, als technisch orientierte Grundlage für darauf aufbauende prozessorientierte Normen gesehen werden. Darin liegt kein Widerspruch, sondern eine Ergänzung auf unterschiedlichen Ebenen. Alle Ebenen, die über der reinen Technik liegen, orientieren sich heute beim BSI genauso an den weltweit anerkannten Normen wie der ISO-2700x-Familie.

3.3.1 ISO-2700x-Reihe

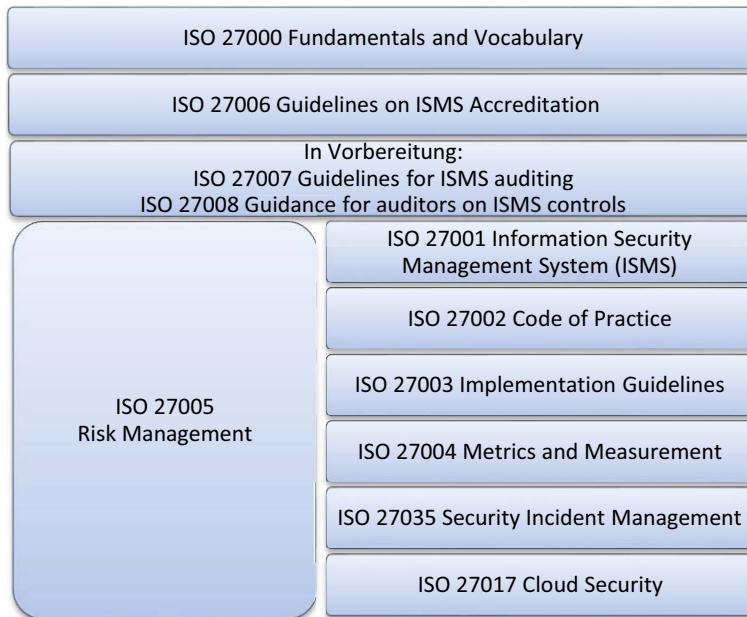
Der Umbau und die Ergänzung der ISO-2700x-Reihe werden langfristig in den Standards 27000 bis 27019 und 27030 bis 27044 münden. Die ISO 27001 steht dabei im Mittelpunkt: Sie definiert die verbindlichen Anforderungen an ein Information-Security-Management-System (ISMS) und stellt damit auch die Norm dar, gegen die sich ein Unternehmen zertifizieren lassen kann.

Alle weiteren Standards präzisieren Teilgebiete des IT-Security-Managements und dienen dazu, dem Manager IT-Security praktische Anleitungen an die Hand zu geben. Neben der ISO-27001- bietet auch die ISO-27000-Norm einen Überblick und erklärt die fundamentalen Zusammenhänge.

Allen Normen der ISO-2700x-Reihe ist gemeinsam, dass sie in Hinblick auf eine Anwendung in jeder Art von Unternehmen mit jeder Größe erstellt wurden. Dementsprechend beschreiben sie eher Prozesse als technische Details. Zudem lassen sie einen erheblichen Spielraum für die Umsetzung der vorgeschlagenen Vorgänge. Ein Beispiel ist das IT-Risikomanagement. Dass es erforderlich ist und damit eine »Muss-Anforderung« darstellt, wird in der ISO 27001 deutlich gemacht. Auf welche Art es allerdings umgesetzt wird, bleibt der IT-Security-Organisation überlassen.

So wird in der ISO 27005 eine Methodik zum IT-Risikomanagement beschrieben, verbindlich genutzt werden muss sie dennoch nicht. Solange die Intention und die Sinnhaftigkeit einer Vorgehensweise dargelegt werden kann, ist auch bei einer Zertifizierung die Art des Weges Sache des Unternehmens. Auch wenn es anerkanntermaßen sinnvoll ist, alle ISO-2700x-Normen als Grundlage für das eigene IT-Security-Management zu nutzen, ist es also durchaus akzeptabel, auch andere Standards wie die des BSI heranzuziehen.

Wie in Abbildung 3.2 ersichtlich, werden in den Normen ISO 27000 und ISO 27006 die Randbedingungen für die Sprache und Begrifflichkeiten auf der einen Seite und die Vorgehensweise bei der abschließenden Zertifizierung eines Unternehmens auf der anderen Seite behandelt.



3

Abbildung 3.2: ISO-2700x-Reihe

Die Thematik Risikomanagement ist ein zentrales Thema, dessen Methodik in beinahe allen Einzelnormen Einfluss findet. Sie ist die Grundlage für die Messung von Sicherheit, für die Priorisierung von Maßnahmen oder für die Bildung eines Überblicks über den aktuellen Stand der Gefährdungslage. Aus diesem Grund wird das Risikomanagement gerne als Werkzeug betrachtet, ähnlich wie der Einsatz der Plan-Do-Check-Act-Vorgehensweise, die bereits in der ISO-9001-Norm von grundlegender Bedeutung ist und den Ansatz zur kontinuierlichen Verbesserung im Rahmen eines geschlossenen Vorgehenskonzepts beschreibt.

Geschichte

Bereits im Jahr 1995 wurde die Norm BS 7799:1995 durch das British Standard Institute veröffentlicht. Ziel war es, die bereits allgemein akzeptierten Best Practices im Bereich der Informationssicherheit zu untersuchen und in einem Werk zusammenzufassen. Im Jahr 1999 wurde die Norm in zwei Teile aufgespalten. Der erste Teil, die BS 7799-1:1999 mit dem Titel »Information Security-Management – Code of Practice for Information Security-Management Systems« stellt einen Leitfaden dar, der beschreibt, wie ein IT-Security-



Management implementiert werden kann. Der zweite Teil, die BS 7799-2:1999, trägt den Titel »Information Security-Management – Specification for Information Security-Management Systems« und beschreibt, welche Anforderungen an die Implementierung und den Betrieb eines Information-Security-Management-Systems (ISMS) gestellt werden. Mit diesen beiden Normen wurde die Grundlage für die heutigen 2700x-Normen gelegt. Durch die Trennung in einen Teil, der als Leitfaden dient, und einen Teil, der verbindlich definiert, welche Anforderungen an ein ISMS zu stellen sind, wurde außerdem die Grundlage für die Möglichkeit zur Zertifizierung gelegt.

Ein Jahr später übernahm die International Standardization Organisation (ISO) den ersten Teil der Norm und setzte sie als ISO 17799:2000 um. Wiederum zwei Jahre später wurde der zweite Teil als BS 7799-2:2002 herausgegeben.

Die aktuelle Version der ISO 27001 aus dem Jahr 2013, deshalb die vollständige Bezeichnung »ISO/IEC 27001:2013«, hat sich aus diesem zweiten Teil heraus entwickelt, die Inhalte der ISO 17799 sind heute als ISO 27002:2013 zu finden. Schaut man sich die Normenkataloge der großen Anbieter an, dann wird seit 2013 eine Reihe an ISO-27001-Normen mit fortlaufenden Jahreszahlen angeboten. Bei der ISO 27001:2015 z.B. handelt es sich um die in die deutsche Sprache übersetzte Version ISO 27001:2013. Die Version ISO 27001:2017 ist wiederum die deutsche Übersetzung der englischen Version ISO 27001:2015, die wenige, leichte Korrekturen enthält. Allgemein anerkannt ist aber weiterhin die ISO 27001:2013 als die aktuelle, maßgebliche Norm.

ISO 27001

Eine herausragende Stellung im Umfeld der 2700x-Normen nimmt die ISO 27001 ein. Sie definiert die Anforderungen an die Zertifizierung eines Information-Security-Management-Systems (ISMS), das als zentrales Framework im Mittelpunkt des normierten Informationsschutzes steht. Ein ISMS stellt im Grunde ein Dokumenten- und Prozessmanagementsystem dar, das dem Zyklus des Plan-Do-Check-Act (PDCA) unterworfen ist. Die vier Stationen des PDCA-Zyklus beschreiben die Stationen Planung des ISMS, Durchführung und Betrieb des ISMS, Überprüfung des ISMS und im letzten Schritt die Instandhaltung und Verbesserung des ISMS. Alle vier Phasen führen zusammen zu einem funktionsfähigen Betrieb eines IT-Security-Managements und



werden in der ISO 27001 abgehandelt. Konzepte wie z.B. das Risikomanagement oder das Messen anhand von Kennzahlen werden angerissen und in der ISO 27004 bzw. ISO 27005 detaillierter aufgeschlüsselt.

In der praktischen Arbeit stehen die ISO 27001 und die ISO 27002 im Mittelpunkt, alle weiteren Normen der ISO-2700x-Familie dienen dazu, offene Fragen hinsichtlich der Vorgehensweise zu beantworten und damit einen Gesamtstandard zur Verfügung zu stellen, der stringent und vollständig beschrieben ist, der objektiv abgearbeitet und zertifiziert sowie in allen Arten von Unternehmen umgesetzt und betrieben werden kann.

3

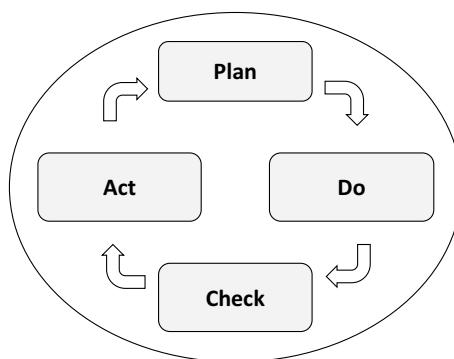


Abbildung 3.3: Plan-Do-Check-Act-Zyklus

Die Möglichkeit, ein Unternehmen oder einen Unternehmensbereich nach ISO 27001 zertifizieren lassen zu können, ist deshalb möglich, weil die Norm von vornherein in diese Richtung ausgelegt ist. Es werden klare Anforderungen aufgestellt, auf unscharfe Formulierungen wird verzichtet. Der Sprachgebrauch hebt sich deutlich von anderen Normen wie z.B. der ISO 27002 ab. Dort ist von Maßnahmen die Rede, die umgesetzt werden *sollten*. Im Rahmen der ISO 27001 ist stets davon die Rede, was getan werden *muss*. Der Maßnahmenkatalog im Anhang A ist zwar, und dies ist der universellen Einsetzbarkeit der Norm geschuldet, wenig detailliert gehalten und nur eingeschränkt technisch orientiert, deckt aber den allergrößten Teil der Arbeitsgebiete der IT-Security ab. Die Gliederung macht es zudem einfach, die entsprechenden Maßnahmen verschiedenen Aufgabenbereichen der IT-Security und damit auch den entsprechenden organisatorischen Bereichen zuzuordnen. Auf diese Weise können Arbeitspakete direkt in Richtung IT-Infrastruktur, Zugangsschutz, Netzwerkbetrieb, Personalabteilung oder auch Einkauf adressiert werden.



Bei all den positiv zu bewertenden Punkten sind aber auch Kritikpunkte anzumerken. Diese betreffen vor allem diejenigen Aufgaben im Rahmen der IT-Security, für die es schwerfällt, Theorie und Praxis in Einklang zu bringen. Zwei Themen sollen beispielhaft erwähnt werden: die Dokumentation im Rahmen des ISMS und die Messung des Erfolgs umgesetzter Maßnahme oder von Risiken im Allgemeinen. Innerhalb der Norm gibt es keine Vorgaben, wie Formulare bzw. Dokumente aufgebaut sein sollen. Es wird zwar in vielen Fällen von Dokumentation gesprochen und welche Anforderungen an die Zurverfügungstellung derselben gestellt werden, doch eine Hilfestellung, wie dies mit elektronischen Mitteln umgesetzt werden soll, fehlt. Dies dürfte einer der Gründe sein, warum es auf dem Markt nur relativ wenige Softwareprodukte gibt, die sich mit dieser Problematik auseinandersetzen, und diese Produkte weichen, wenn man sie miteinander vergleicht, stark voneinander ab. Das führt dazu, dass selbst in den ganz großen Unternehmen noch immer die Nutzung von Excel vorherrscht, wenn es um ein ISMS-Tool geht.

Der zweite Themenblock bezieht sich darauf, dass ein kontinuierliches Verbesserungssystem wie der PDCA-Zyklus im Wesentlichen davon lebt, dass einmal implementierte Maßnahmen laufend daraufhin untersucht werden, ob sich der erwartete Erfolg einstellt oder nicht. Tut er dies nicht, so sind Verbesserungen in Prozessen, Vorgehensweisen und eventuell Richtlinien erforderlich. Nur wie misst man den Erfolg von Maßnahmen, also von Arbeiten, die jemand im Rahmen seiner Tätigkeit erbringt oder die von IT-Systemen erbracht werden? Jede Antwort auf diese Frage wird schnell in einen sehr technischen Bereich abgleiten müssen, da im Endeffekt vor allem Bits und Bytes miteinander verglichen werden können. Dies in einer weiteren Norm vorzugeben, ist schwierig, und dementsprechend oberflächlich ist die dazugehörige ISO 27004 »ISMS Metrics and Measurement« gehalten.

ISO 27002

Ziel der ISO 27002 ist die Beschreibung eines Rahmenwerks für das IT-Security-Management. Wie der Name »Information Technology – Code of Practice for Information Security-Management« schon aussagt, befasst es sich hauptsächlich mit Maßnahmenzielen, die angerissen werden und dabei kaum in die Tiefe gehen. Damit sind sie eher als Übersicht zu sehen. Die Umsetzung



KAPITEL 3 – IT-COMPLIANCE

der beschriebenen Maßnahmenziele und die Etablierung eines funktionierenden IT-Security-Prozesses sind eine Möglichkeit, die Anforderungen der ISO 27001 umzusetzen.

Hinweis

Der Begriff »code of practice«, also »Leitfaden«, betont den Unterschied zur ISO 27001, die konkrete Anforderungen aufstellt. Aus diesem Grund ist eine Zertifizierung nach ISO 27002 nicht möglich.

3

Der lange Entwicklungsprozess und die vielen Einflüsse verschiedener Best-Practice-Schriften spiegeln sich in den realitätsnahen Maßnahmenzielen wider, die in der ISO 27002 zusammengefasst sind. In den letzten Jahren sind immer mehr Unternehmen dazu übergegangen, den IT-Security-Ansatz dieser Norm zu adaptieren und die internen Prozesse dahin gehend auszurichten. Dies beweist zum einen das steigende Bewusstsein für IT-Security und zum anderen den Stellenwert, den diese Norm genießt.

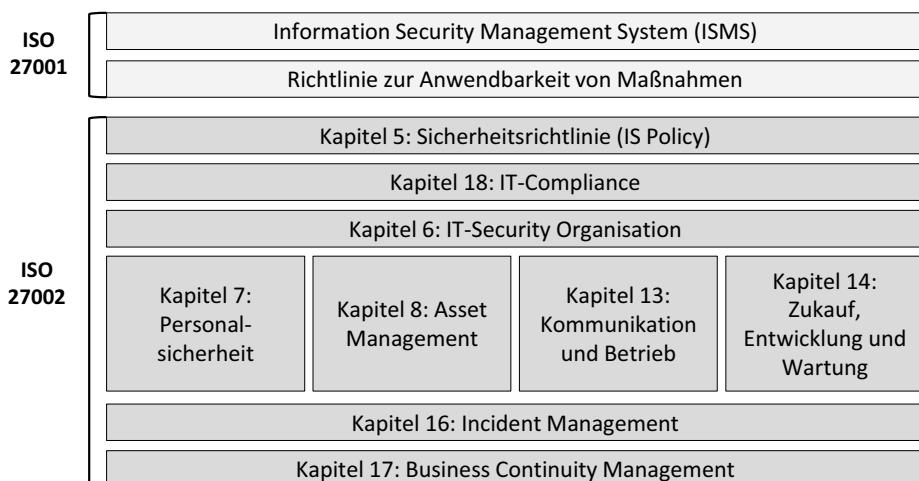


Abbildung 3.4: Zusammenspiel ISO 27001 und ISO 27002

Die im Leitfaden aufgeführten Maßnahmen helfen, den Level der IT-Security in einem Unternehmen nachhaltig zu erhöhen. Sie beziehen sich dabei nicht nur auf IT-Systeme und IT-Equipment, sondern auch auf sensible Bereiche



wie die Personalabteilung oder den Einkauf. Neben Daten in elektronischer Form wird auch auf Daten in Papierform eingegangen.

3.3.2 Standards des Bundesamts für Sicherheit in der Informationstechnik

Die am häufigsten zitierte und auch am häufigsten in den Unternehmen eingesetzte Veröffentlichung des Bundesamts für Sicherheit in der Informationstechnik (BSI) war von 1994 bis 2005 das IT-Grundschutzhandbuch. Keine andere Publikation hat in Deutschland so umfangreich und ausführlich Bezug auf konkrete Sicherheitsmaßnahmen für eine so große Bandbreite an IT-Systemen und Softwareprodukten geboten. Selbst in einer sehr heterogen aufgebauten IT-Infrastruktur konnten Beschreibungen für die Konfiguration von Betriebssystemen, den Aufbau und Einsatz von Hardware und Maßnahmen für den Betrieb von Rechenzentren gefunden werden.

Ab 2005 wurde das IT-Grundschutzhandbuch in die Bereiche BSI-Standards zur Informationssicherheit und IT-Grundschutz-Kataloge unterteilt. Die Unterteilung wird in Abbildung 3.5 dargestellt.

3

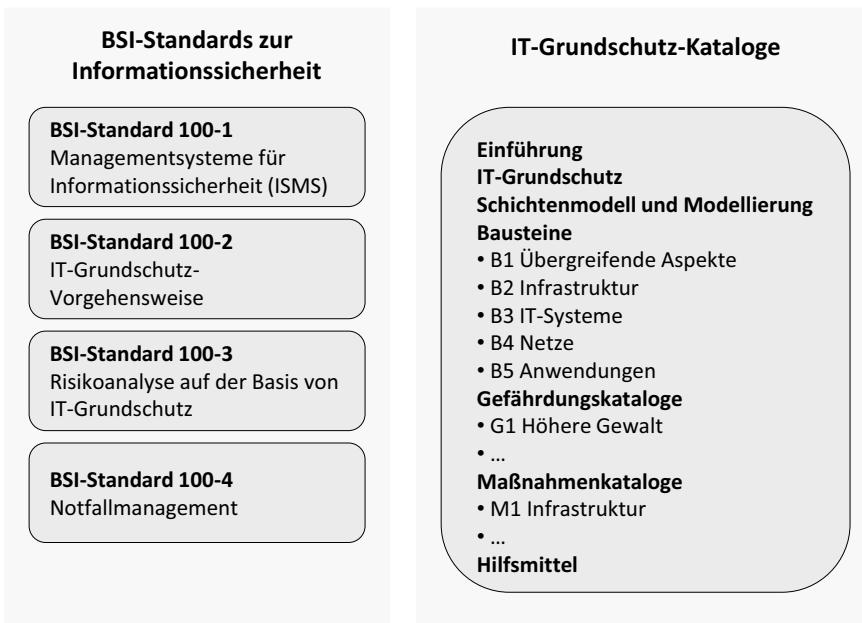


Abbildung 3.5: Standards des BSI



Im Gegensatz zu den technisch orientierten IT-Grundschutz-Katalogen sind die BSI-Standard-Dokumente in sich thematisch geschlossen und beschreiben Vorgehensweisen, wie mit den jeweiligen Aufgabenbereichen organisatorisch und methodisch umzugehen ist.

BSI-IT-Grundschutz-Kataloge

In den IT-Grundschutz-Katalogen finden sich detailliert beschriebene Maßnahmen, deren Umsetzung einen angemessenen Grundschatz gewährleisten. Die in den Katalogen aufgeführten Beschreibungen erstrecken sich über eine Vielzahl von Betriebssystemen und Applikationen bis hin zu Empfehlungen hinsichtlich der Nutzung von Hardware. Dementsprechend stark sind die Kataloge laufenden Änderungen unterworfen. Neue Systeme erfordern neue Konfigurationsbeschreibungen, während ältere Versionen mit der Zeit ausgesondert werden.

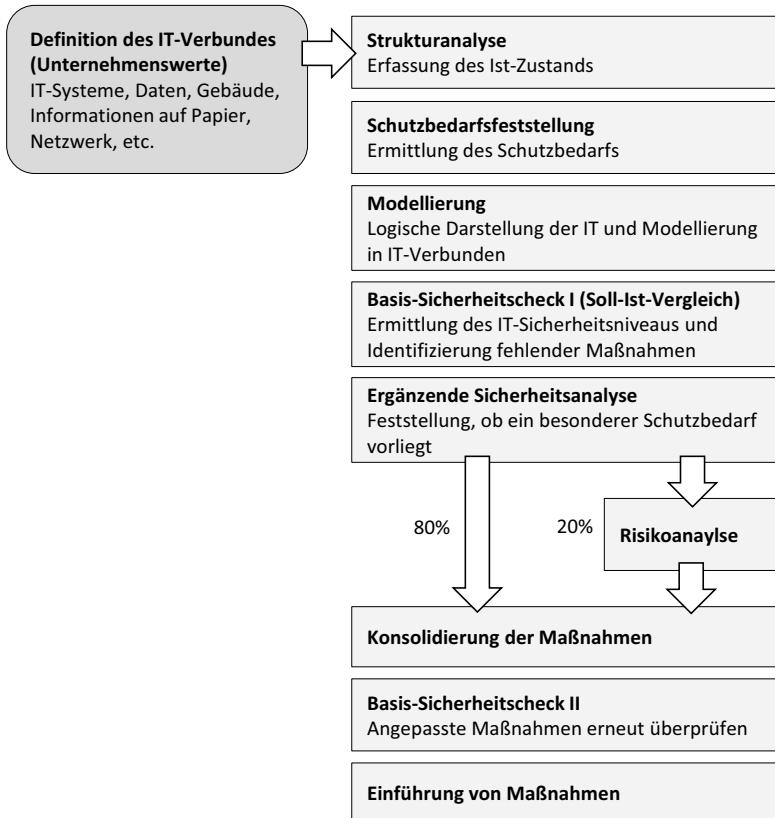
3

Tipp

Auch wenn einige Software-Plattformen nicht weiter gepflegt werden, ist es dennoch immer noch sinnvoll, die eigenen Systemvorgaben mit denen der Kataloge zu vergleichen. In einigen Fällen ist es auch möglich, ganz auf eigene technische Konfigurationshandbücher zu verzichten und stattdessen auf die Richtlinien des BSI zu verlinken.

Der Zugriff auf die Beschreibungen des BSI ermöglicht es dem Administrator, ohne eigene Recherche einen Großteil an Antworten auf seine Sicherheitsanforderungen zu finden. Natürlich geschieht dies zunächst auf technischer Ebene. Zusätzlich werden aber auch Bedrohungskataloge und daraus resultierende organisatorische und infrastrukturelle Maßnahmen mitgeliefert. Für Systeme, bei denen der Einsatz in kritischen Umgebungen oft vorkommt bzw. auf denen üblicherweise sensible Daten verarbeitet werden, werden häufig auch über das normale Sicherheitsmaß hinausgehende Maßnahmen vorgeschlagen.

Laut eigenen Angaben können über den Weg Grundschutz ca. 70 % aller zu bearbeitenden Assets abgehandelt werden. Weitere 30 % werden entweder nicht vollständig erfasst oder aber ihr Sicherheitsbedarf ist höher als normal, und infolgedessen wird zusätzlich eine Risikoanalyse gestartet mit dem Ziel, weitere zielgerichtete Maßnahmen zu definieren.



3

Abbildung 3.6: Vorgehensweise nach BSI-Grundschutz-Katalogen

Hinweis

Die Abhängigkeit des Einsatzes eines IT-Risikomanagements von der Kritikalität ist der größte Unterschied zwischen den Ansätzen des BSI und den ISO-27001-Normen, bei denen in jedem Fall ein IT-Risikomanagement stattfinden muss.

BSI-100-1-Managementsysteme für Informationssicherheit

Im BSI-Dokument 100-1 zeigt sich die seit 2005 bestehende Nähe zum ISO-27001-Standard besonders stark. Die Einführung und der Betrieb eines Information-Security-Management-Systems werden darin aufgezeigt und bleiben dabei stets kompatibel zur ISO-Norm. Um den Zusammenhang vor Augen zu



KAPITEL 3 – IT-COMPLIANCE

führen, wurden typische Bezeichnungen entweder direkt übernommen oder zumindest erwähnt. In dieser für das IT-Security-Management grundlegenden Norm wurde darauf verzichtet, einen Sonderweg einzuschlagen, und nur dadurch kann eine Zertifizierung nach »ISO 27001 auf Basis von IT-Grundschutz« auch international bestehen.

Für den Manager IT-Security stellt sich damit die Frage, welches Dokument er als Basis nutzen soll, und zwar unabhängig davon, ob er eine Zertifizierung anstrebt oder nicht. Wie so häufig liegt die Antwort im Selbstverständnis der eigenen IT-Security-Organisation. Je mehr ein ISMS auch die detaillierte, technische Umsetzung von Maßnahmen begleiten soll, desto wertvoller werden die IT-Grundschutz-Kataloge des BSI sein und desto sinnvoller ist es, von vornherein den Weg einzuschlagen, den das BSI aufzeigt. Beim Vergleich der Normen zeigen sich zudem der oft pragmatischere Ansatz und die stringenteren Methodenbeschreibung der BSI-Standards. Der ursprüngliche Ansatz, einem IT-Administrator durch eine einfache, aber tief gehende Beschreibung zur Seite zu stehen, wird an dieser Stelle weitergeführt. Noch deutlicher als im BSI-Standard 100-1 wird dies in den weiteren BSI-Standards, die sich zum Teil deutlicher von den ISO-Normen abheben.

3

BSI-100-2-IT-Grundschutz-Vorgehensweise

Werden im BSI-Standard 100-1 noch die generell erforderlichen Komponenten eines IT-Security-Managements bzw. des ISMS aufgezählt, so wird im Standard 100-2 die grundsätzliche Einführung an sich abgearbeitet. Die Grundlage bilden wiederum die IT-Grundschutz-Kataloge, die auf IT-Systeme, Software und andere Komponenten der Geschäftsprozesse Anwendung finden.

BSI-100-3-Risikoanalyse

Ein großer Unterschied zwischen der BSI-Vorgehensweise und dem ISO-Regelwerk ist der Umgang mit IT-Security-Risiken. Müssen Risiken dem BSI-Standard 100-3 folgend nur bei Unternehmenswerten mit erhöhtem Schutzbedarf durch ein Risikomanagement bearbeitet werden, so ist dies bei der entsprechenden ISO-27001-Norm die grundlegende Methodik zur Erkennung, welche Maßnahmen sinnvoll eingesetzt werden sollten. Dahinter liegt der Gedanke, dass eine Vorgehensweise auf Basis der IT-Grundschutz-Kataloge bereits eine hinreichende Beurteilung des Schutzbedarfs inklusive der Implementierung von abgeleiteten Maßnahmen und deren Verfolgung beinhaltet.



BSI-100-4-Notfallmanagement

Schon in den Bausteinen der IT-Grundschutz-Kataloge wird die Notfallvorsorge als wichtiger Punkt behandelt. Die Umsetzung der dort aufgeführten Vorgaben beinhaltet die Definition von Verantwortlichen, die Notfallvorsorge, den Weiterbetrieb der betroffenen Prozesse durch geeignete Notfallszenarien oder Verwendung von Backups und die Wiederherstellung.

Der BSI-Standard 100-4 geht darüber hinaus explizit auf die Prozesse des Notfallmanagements ein und bildet damit einen größeren Rahmen ab, innerhalb dessen eine Strukturierung des Gesamtaufgabenfelds stattfindet. Ein Manager IT-Security, der innerhalb eines IT-Security-Managementprozesses die Aufgabe hat, sich um die Verfügbarkeit von IT-Systemen zu kümmern, kann mit diesen Hilfestellungen ein IT (Business) Continuity Management aufbauen. Zusätzlich zu den losen und unsortierten Bausteinen der IT-Grundschutz-Kataloge werden damit ein zeitlicher Ablaufplan, erforderliche Dokumente wie ein Alarmierungsplan und der kontinuierliche Verbesserungsprozess hinzugefügt. Insbesondere Letzterer macht aus einem Notfallplan ein Notfallmanagement und schafft dadurch Schnittstellen zum ISMS und den dort beschriebenen Phasen Plan-Do-Check-Act, indem ein Notfallmanagement-Lifecycle gegenübergestellt wird.

BSI-Anforderungskatalog Cloud Computing C5

Mit der Veröffentlichung des C5-Cloud-Computing-Katalogs trägt das BSI dem immer weiter verbreiteten Auslagern von Software, Datenspeicherung und Datenverarbeitung hin zu Public-Cloud-Anbietern Rechnung. Die im Katalog aufgeführten Anforderungen richten sich zunächst an die Anbieter selbst. Diejenigen Unternehmen, die einen solchen Dienst beauftragen, können sich diese Anforderungen wiederum zu eigen machen und in ihre Verträge integrieren. Das Werk ist eingebettet in bereits bestehende Prozessbeschreibungen wie denen der ISO 27001 oder anderen Standardisierungsgremien und harmoniert deshalb auch gut mit einem bereits betriebenen ISMS.

3.3.3 Gegenüberstellung ISO 2700x und BSI-Grundschutz

In den vorigen Abschnitten hat es sich bereits herauskristallisiert: Beide Normenfamilien sind gleichermaßen geeignet, in einem Unternehmen das IT-Security-Management zu begleiten, zu strukturieren und letztendlich auch in Form einer Zertifizierung abzunehmen. Der Ansatz des BSI stammt aus dem



sehr stark technisch detailliert geprägten Umfeld, während der ISO-Ansatz eher prozessorientiert ist. Für ein klareres Bild fasst die folgende Tabelle die wesentlichen Unterschiede der Normen zusammen.

	BSI-Grundschutz	ISO 2700x
Internationale Verbreitung	Das Bundesamt für Sicherheit in der Informationstechnik ist eine deutsche Behörde und stellt als solche die Normen kostenfrei zur Verfügung. Im Internet können unter www.bsi.de die Dokumente und zusätzlich einige hilfreiche Applikationen heruntergeladen bzw. bestellt werden.	Die ISO 27001 ist, nicht zuletzt aufgrund ihres Alters, weltweit verbreitet und sehr gut anerkannt. Die Anzahl an Zertifizierungen steigt zunehmend, ohne dass die Vergleichbarkeit der einzelnen Zertifizierungen in größerem Maße schwankt. Gremien wie der Verband der Automobilindustrie (VDA) bauen auf dem Standard ihr eigenes Audit-System (TISAX) auf und gliedern ihren Fragekatalog auf Basis der Maßnahmen aus Anhang A der ISO 27001.
	Ein Grund für die Anlehnung an die ISO 27001 war das Ziel der weltweiten Akzeptanz insbesondere für die Zielgruppe weltweit agierender Unternehmen. Trotzdem steht die Norm diesbezüglich weiterhin im Schatten der ISO 27001.	Das Regelwerk kann in deutscher Sprache bestellt werden.
Aufbau und Inhalt	Die IT-Grundschutz-Kataloge gehen auf mehreren Tausend Seiten bis ins technische Detail von IT-Systemen und Softwarekonfigurationen. Daraus kann der Handbuchcharakter der Kataloge ersehen werden. Die BSI-Standards dagegen sind zwar pragmatischer gehalten als die korrespondierenden ISO-2700x-Normen, aber weitgehend deckungsgleich und erfüllen den gleichen Zweck.	Die Normen müssen unabhängig von Unternehmenszweck und Unternehmensgröße einsetzbar sein und sind dementsprechend allgemein gehalten. Sie beschreiben Methoden und Anforderungen und sind, abgesehen von der ISO 27002, kurz gehalten.



	BSI-Grundschutz	ISO 2700x
	Insgesamt ca. 1.200 Maßnahmen und ca. 500 Bedrohungen werden aufgeführt.	Insgesamt 114 Maßnahmen werden in ISO 27001 Anhang A beschrieben.
Vorgehensweise	Die BSI-Standards gehen methodisch vor, setzen aber jederzeit den technischen, maßnahmenorientierten Unterbau der IT-Grundschutz-Kataloge voraus.	Der Ansatz ist prozessorientiert und beschreibt die Etablierung eines kontinuierlichen Verbesserungsprozesses mit dem Ziel, das angestrebte Sicherheitsniveau zu erreichen.
IT-Risikomanagement	Der IT-Risikomanagementprozess ist für Assets mit erhöhtem Schutzbedarf erforderlich. Grundsätzlich sind neben dem BSI-Standard 100-3 auch andere Risikomanagementansätze einsetzbar. Dies wird aber nicht empfohlen.	Der IT-Risikomanagementprozess ist für alle Assets durchzuführen. Grundsätzlich ist zu empfehlen, den Ansatz der ISO 27005 zu wählen. Im Prinzip ist aber auch eine andere Vorgehensweise zulässig, muss aber im Rahmen einer Zertifizierung schlüssig erläutert werden können.
IT (Business) Continuity Management	BCM, im Sprachgebrauch des BSI »Notfallmanagement«, ist sowohl in den IT-Grundschutz-Katalogen integriert als auch explizit im BSI-Standard 100-4 beschrieben.	BCM spielt in der ISO 27001 eine eher untergeordnete Rolle, da dieser Bereich eher dem IT-Betrieb zugesprochen wird. Wert wird aber auf die Wiederherstellung nach einer Cyber-Attacke gelegt.
Zertifizierung	Das implementierte ISMS und die dazugehörigen Prozesse müssen nachweisbar im Betrieb funktionieren. Ist dies der Fall, dann kann sechs Monate nach Einführung eine Zertifizierung stattfinden.	Nach Einführung eines ISMS nach ISO 27001 muss zunächst der Nachweis erbracht worden sein, dass alle Stufen des Plan-Do-Check-Act-Zyklus im Betrieb gelebt werden. Dies wird allgemein frühestens nach einer Frist von sechs Monaten angenommen. In diesem Zeitpunkt sollte es auch keine wesentlichen Änderungen am Scope der Zertifizierung geben. Danach ist eine Zertifizierung möglich.



	BSI-Grundschutz	ISO 2700x
	Das Zertifikat ist für drei Jahre gültig und kann danach verlängert werden.	Eine Zertifizierung ist für drei Jahre gültig und muss danach verlängert werden.

3.3.4 ITIL

Die IT Infrastructure Library (ITIL) hat sich über die letzten Jahre als Bibliothek einer Reihe von international anerkannten Verfahren auf ihrem Gebiet etabliert. Sie beschreibt im Rahmen von sechs »Büchern«, wie die Organisation von IT-Steuerungsprozessen gestaltet werden kann. Sie hilft dabei, von der technischen Ebene hin zu einer Prozesssicht zu abstrahieren, ohne den Kontakt zu den IT-Systemen zu verlieren. Die wesentlichen Perspektiven, aus denen auf den IT-Betrieb geblickt wird, sind dabei die Servicesicht und die Prozesssicht.

Tipp

Die Bücher und weiterführende Publikationen rund um ITIL sind frei verfügbar. Einige Werke sind zudem in deutscher Sprache erhältlich.

Das Ziel sind sichere, verfügbare und integre IT-Dienstleistungen und damit decken sich die Schutzziele der IT-Security mit denen von ITIL. Wie bei anderen ganzheitlichen Managementsystemen bedeutet das hier, dass eine strenge Organisation und Dokumentation von IT-Prozessen den sicheren Umgang mit Daten und IT-Systemen fördert. Insbesondere in der Phase der Neustrukturierung oder Umstrukturierung von Prozessen nach ITIL hat der Manager IT-Security die Möglichkeit, die Belange des Informationsschutzes mit einfließen zu lassen. Er kann dabei auf den Bereich »Service Continuity Management« verweisen, innerhalb dessen die Thematik IT-Security definiert wird. Auch der Verweis auf die konkrete Sicherheitsnorm BS 7799 ist dort enthalten, die wiederum die Grundlage für die ISO 27002 bildet.

Neben der grundsätzlichen Definition von IT-Security und den damit verbundenen Zielen wird das Gebiet auch in den verschiedenen Büchern wiederholt angesprochen. Als Grundlage für ein unternehmensweit durchgängiges IT-Security-Management ist dies aber bei Weitem nicht ausreichend.



ITIL in der aktuellen Fassung enthält kein eigenes Informationssicherheitsmanagement, sondern bietet die Möglichkeit, über Schnittstellen ein parallel dazu betriebenes Informationssicherheitsmanagement nach ISO 27001 anzubinden.

3.3.5 Weitere Standards

Neben den aufgeführten Normen sind viele weitere verfügbar, die entweder die IT-Security aus einem anderen Blickwinkel betrachten oder aber in Teilgebieten wichtige Hilfestellungen bieten. Als Erstes sind alle Standards der 2700x-Reihe zu erwähnen, die nicht explizit aufgeführt wurden. Jeder IT-Security-Spezialist ist gut beraten, hinsichtlich dieser Reihe auf dem Laufenden zu bleiben und Neuerscheinungen aufmerksam zu studieren. Vor allem die Normen zum IT-Risikomanagement (und da sind neben der ISO 27005 auch explizit die ISO 31000 und die ISO 31010 zu erwähnen) sind sehr wichtig für das Verständnis, auf welche Art die Betrachtung von Risiken Teil des IT-Security-Prozesses sein kann. Zur Quantifizierung von Risiken wiederum dient die ISO 27004, die sich mit Kennzahlen beschäftigt und sie in einen Kontext mit dem Plan-Do-Check-Act-Regelkreis bringt. Das reicht von der Auswahl von Kennzahlen und der Zuweisung zu den entsprechenden Maßnahmen über die Implementierung bis hin zur Auswertung und Nutzung der Ergebnisse für Verbesserung. Wie alle ISO-2700x-Normen ist auch diese Norm eher allgemein gehalten, bietet aber sehr wertvolle Hinweise zur Handhabung von Kennzahlen innerhalb einer heterogenen Infrastruktur.

Eine weitere wichtige Norm ist der ISO-Standard zur Meldung von Sicherheitereignissen. Die dazugehörigen Vorgaben sind in der ISO 27035 zusammengefasst. Diese wurde im Jahr 2016 in zwei Teile aufgesplittet. Zum einen die ISO 27035-1:2016 mit dem Titel »Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management«, die sich mit den grundsätzlichen Zusammenhängen eines Meldesystems von Sicherheitsvorfällen beschäftigt, und die ISO 27035-2:2016 mit dem Titel »Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response«, die, wie es der Titel schon sagt, das Management von Sicherheitsvorfällen behandelt.

Neben den Normen, die sich direkt mit der IT-Security befassen, sind weitere Normen hilfreich. Als Erstes zu nennen sind die Standards ISO 15504, die ein



Fortschrittssystem mitbringt, das sich wiederum im Rahmen der Kennzahlen nutzen lässt, und die ISO 15408 Common Criteria, die, wie der Name schon sagt, ein System zur Bewertung der IT-Security vorgibt.

Daneben gibt es viele weitere Normen, die sich mit physischen Sicherheitsbelangen befassen. Dazu gehören z.B. Bauvorschriften, die genau regeln, wie feuerfeste Türen oder einbruchssichere Fenster auszusehen haben. Viele sind als DIN-Normen verfügbar und stellen sicher, dass man den adäquaten Schutz für den entsprechenden Unternehmenswert bereitstellt.

3.4 Gesetze

3

Ungeachtet der Tatsache, dass keine konkrete gesetzliche Anforderung existiert, IT-Security-Management zu betreiben, gibt es zahlreiche gesetzliche Vorschriften, die in viele Teilgebiete der IT-Security hineinspielen. Das reicht vom Strafgesetzbuch mit dem Paragrafen, der sich mit der Sabotage von Computern auseinandersetzt, bis hin zu Maßnahmen, die aus dem Sarbanes-Oxley Act (SOX) abgeleitet werden können. Die Vielzahl an einzelnen Vorschriften verteilt sich auf Dutzende Gesetze, und weitere Hunderte von Urteilsbegründungen aus Gerichtsurteilen zu dieser Thematik runden das Thema ab und geben ihm gleichzeitig eine hohe Dynamik.

Die Vielfalt an Gesetzen, die unzähligen Gerichtsurteile und die sich ständig ändernde herrschende Meinung sind Herausforderungen, die gemeistert werden müssen. Dies lässt sich am einfachsten dadurch erreichen, dass man zunächst auf Basis des eigenen gesunden Menschenverstands handelt. Dann erkennt man auch ohne Kenntnis der jeweiligen Gesetzeslage schnell, dass es nicht in Ordnung sein kann, wenn personenbezogene Daten ohne entsprechenden Schutz verarbeitet werden, oder dass die Nachvollziehbarkeit von administrativen Handlungen im Zweifelsfall wichtig werden kann. Wenn man dazu die entsprechende Presse verfolgt und sich auf die wichtigsten Gesetze konzentriert, dann ist man bereits auf einem guten Weg.

In erster Linie gibt die EU-Datenschutz-Grundverordnung (EU-DSGVO) vor, wie mit personenbezogenen Daten umgegangen werden muss. Dieses Gesetz beschränkt sich dabei auf Informationen, die elektronisch verarbeitet werden, und auf diejenigen, die aus Sicht des Gesetzes schutzwürdig sind. Da es sich dabei aber um einen großen Teil aller Daten handelt bzw. sich unter allen Arten von Daten häufig auch ein personenbezogenes Datum befinden kann, hat es großen Einfluss auf Maßnahmen und Prozesse des IT-Security-Managements.



3.4.1 EU-Datenschutz-Grundverordnung

Ein großer Teil der Daten in einem Unternehmen beinhalten auch personenbezogene Informationen. Oft handelt es sich dabei um Namen und Adressen. Manchmal aber auch um Informationen, die erst in Kombination mit anderen Daten auf die Arbeitsleistung oder Einstufung eines Mitarbeiters schließen lassen. Die Grenze zwischen Daten, die auf Basis der EU-DSGVO behandelt werden müssen oder nicht, ist schwierig zu greifen und oft nur im großen Zusammenhang erkennbar. Daraus kann man leicht ersehen, dass keine klare Trennung von Datensicherheit und Datenschutz möglich ist.

Ein weiterer Grund liegt in der Vergangenheit begründet. Der klassische Datenschutz hat sich meist mehr mit den juristischen Details denn mit der technischen Verarbeitung von Daten beschäftigt. Das ist aber ungenügend. Die Verbindung zum Informationsschutz schafft die EU-DSGVO selbst, da sie direkten Bezug zu den Schutzmechanismen der ISO 27001 nimmt und sowohl deren Schutzziele »Vertraulichkeit«, »Verfügbarkeit« und »Integrität« übernimmt, als auch den Mechanismus des Risikomanagements. Die Schutzziele sind dabei durch Maßnahmen zu erreichen, die dem »Stand der Technik« entsprechen. Damit legt dieses Gesetz die Messlatte sehr hoch und insbesondere diese Formulierung lässt aktuell noch sehr viel Spielraum für Interpretationen.

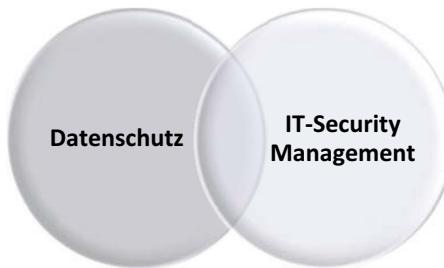


Abbildung 3.7: Spannungsfeld zwischen IT-Security und Datenschutz

Die EU-DSGVO beinhaltet eine Reihe an Öffnungsklauseln, die länderspezifisch in eigenen Gesetzen näher ausgeführt werden können. In Deutschland wurde dazu das Bundesdatenschutzgesetz-Neu veröffentlicht. In diesem Gesetz werden die Technisch-Organisatorischen Maßnahmen, die es bereits im Bundesdatenschutzgesetz-Alt gab, neu aufgegriffen und leicht angepasst veröffentlicht. Im Bundesdatenschutzgesetz-Neu sind diese Maßnahmen in § 64 aufgeführt. So wird die Zutrittskontrolle nun der Zugangskontrolle zuge-



schlagen und es wurden neue Kontrollen hinzugefügt wie die Wiederherstellbarkeit, die Zuverlässigkeit und die Datenintegrität.

Das Bundesdatenschutzgesetz-Neu § 64 (1) gibt den Umfang und die Qualität der technischen Maßnahmen vor, die getroffen werden müssen, um personenbezogene Daten zu schützen. Insbesondere heißt es hier: »Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten [...].« Des Weiteren wird auf die Rolle des Bundesamts für Sicherheit in der Informationstechnik (BSI) hingewiesen, deren Empfehlungen zu berücksichtigen sind. Ab § 64 (3) werden die einzelnen Technisch-Organisatorischen Maßnahmen vorgestellt, die in der folgenden Tabelle, in Beispielen, den Maßnahmen aus der ISO 27001 und der ISO 27002 gegenübergestellt werden.

Bundesdatenschutzgesetz-Neu § 64	Bezug zur IT-Security und zur ISO 27001 / 27002
Abschnitt (1) Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten [...].	Auch wenn der Einzelpunkt »Organisationskontrolle« des alten Datenschutz-Gesetzes weggefallen ist, so wird es anhand des ersten Abschnitts schnell deutlich, dass die Technik und die Organisation Hand in Hand gehen müssen, um das erforderliche Mindestniveau an Sicherheit gewährleisten zu können. Der »Verantwortliche« – und dabei wird es sich in den meisten Fällen um die Unternehmensleitung handeln – hat dafür Sorge zu tragen, dass beide Punkte den Empfehlungen des BSI folgen.



Bundesdatenschutzgesetz-Neu § 64	Bezug zur IT-Security und zur ISO 27001 / 27002
Abschnitt (2) Das Ziel der unter Abschnitt (1) geforderten Maßnahmen ist die Sicherstellung von »Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste« und darüber hinaus, dass »die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können«.	In der EU-DSGVO werden die Technisch-Organisatorischen Maßnahmen mehr aus dem Blickwinkel der allgemeineren Anforderungen die Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit zu gewährleisten dargestellt. Abschnitt (2) ist damit ein Verweis auf die Verordnung. Alle Abschnitte der ISO 27001 und der ISO 27002 beziehen sich auf diese Schutzziele.
Zugangskontrolle Die Zugangskontrolle vereinigt nun den Zutrittschutz und den Zugangsschutz in einer Technisch-Organisatorischen Maßnahme (TOM). Die darauf abzielenden Maßnahmen umfassen generell den Schutz von physischen Assets mit Bezug zu personenbezogenen Daten. In erster Linie werden das IT-Systeme sein, die z.B. in einem Serverraum untergebracht sind.	Die physische Sicherheit von Unternehmenswerten ist zu gewährleisten. Dabei kann es sich z.B. um den physischen Schutz von IT-Systemen handeln oder auch, genereller ausgedrückt, um den Zutritt zu Sicherheitszonen. Maßnahmen aus Anhang A: A.11
Zugriffskontrolle »Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.«	Die Zugriffskontrolle, also die Vorgabe, dass der Zugriff auf Daten nur durch authentifizierte und dafür autorisierte Personen und Applikationen erfolgen darf, zieht sich wie ein roter Faden durch die ISO 27002 und damit auch durch die Maßnahmen des Anhangs A der ISO 27001. Auch wenn das Thema in A.9 explizit mit Maßnahmen hinterlegt wird, ist es zugleich Bestandteil weiterer Maßnahmen in den unterschiedlichsten Bereichen.



Bundesdatenschutzgesetz-Neu § 64	Bezug zur IT-Security und zur ISO 27001 / 27002
Eingabekontrolle »Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.«	Kontrollen dieser Art werden in der Regel durch die Protokollierung von »wer hat was wann getan« gelöst. Dazu kommt die Ablage der Logdaten auf eine geeignete Art und Weise. Das kann innerhalb einer revisionssicheren Archivlösung geschehen oder aber in einer Blockchain-basierten Datenbank. Maßnahmen aus Anhang A: A.12.4
Transportkontrolle »Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.« Datenträgerkontrolle »Verhinderung des unbefugten Lesens, Kopieren, Veränderns oder Löschens von Datenträgern.«	Die Übertragung von Daten z.B. über ein Netzwerk, auf Datenträgern wie USB-Sticks oder Wechselseitplatten ist allgegenwärtig. Der Schutz der Daten kann z.B. durch eine Kombination von Verschlüsselung und Datensicherung gewährleistet werden. Dazu kommen die Maßnahmen aus dem Bereich der Netzwerk-Sicherheit. Maßnahmen aus Anhang A: A.11, A13 und A.8.3
Wiederherstellbarkeit »Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.« Zuverlässigkeit »Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.«	Daten jederzeit zuverlässig bereitstellen zu können und nach einem Notfall wie einem Sicherheitsereignis wiederherzustellen, ist Bestandteil vieler einzelner Maßnahmen und Teil des grundsätzlichen Schutzzieles der Verfügbarkeit. Explizit wird es in A.17 aufgegriffen. An dieser Stelle werden das Business Continuity Management aus der Sicht der IT-Security betrachtet. Eine weitere direkte Verbindung gibt es zum Thema »Backup« in A.12.3.

Es fällt auf, dass sich viele Kontrollen mit den typischen Schutzzielen der IT-Security decken und damit mit der Aufgabenstellung des Managers IT-Security überschneiden. In Abbildung 3.7 ist dieser gemeinsame Bereich in der überlappenden Zone zwischen dem Datenschutz und dem Informationsschutz dargestellt. Bezeichnen könnte man diesen Bereich als »Security-Management«,



denn es beschreibt die Umsetzung der in der EU-DSGVO vorgeschriebenen Aufgaben durch die Einführung und den Betrieb von technischen Methoden. Diese Techniken werden im Allgemeinen durch den Datenschutzverantwortlichen veranlasst, durch den Manager IT-Security koordiniert und durch die IT-Fachbereiche umgesetzt.

3.4.2 IT-Sicherheitsgesetz

Seit Inkrafttreten des IT-Sicherheitsgesetzes (IT-SiG) im Jahr 2015 sind Unternehmen, die per Gesetz als Betreiber kritischer Infrastrukturen (KRITIS) festgelegt wurden, in den Fokus der Behörden gerückt. Neben den Telekommunikationsunternehmern sind dies vor allem Energieversorger, Transportunternehmen und Versorger. Diese wurden von den Behörden auf ihre besondere Verantwortung hingewiesen – nicht ohne eine klare Deadline für die Implementierung eines ISMS. In nächster Zeit wird die Version 2 dieses Gesetzes erwartet, die voraussichtlich vor allem eine Erweiterung des Kreises der betroffenen Unternehmen bedeuten wird. Wenn die aktuellen Pläne umgesetzt werden, gelten die verschärften Regeln dann auch für viele Unternehmen, die bislang keinem größeren Druck von außen ausgesetzt waren.

3

3.4.3 Weitere Gesetze

Neben den bereits erwähnten Gesetzen, die meist die Unternehmensleitung und deren Verantwortung ansprechen, sind weitere Gesetze für den Informationsschutz relevant. Meistens ist die Erfüllung dieser Gesetze eine Grundlage für die Einführung eines IT-Security-Managements, oft unterstützt ein funktionsfähiges ISMS aber auch deren tägliche Einhaltung.

Die bestehenden sogenannten Multimediagesetze enthalten eine Reihe wichtiger Regelungen, die in vielen Unternehmen anwendbar sind. Unter dem Oberbegriff »Multimediagesetze« verbergen sich u.a. die folgenden Gesetze:

- Telekommunikationsgesetz (TKD): Interessante Paragraphen sind hier unter anderem § 85 II, § 88, § 89, § 91 ff., § 109 und § 113 ff.
- Telemediengesetz (TMG): Das TMG ist ein relativ neues Gesetz, das 2007 veröffentlicht wurde. Es fasst viele Regelungen u.a. des TDG, des TDDSG und des Mediendienststaatsvertrags (MDStV) zusammen. Es ist für jeden interessant, der Leistungen über das Internet erbringt, und enthält viele Vorschriften des Internetrechts.



KAPITEL 3 – IT-COMPLIANCE

Neben den Multimediasetzen sind noch weitere relevante Gruppen an Gesetzen zu nennen. Dazu gehört das Urheberrecht, das im Urheberrechtsgesetz (UrhG) zusammengefasst ist. Dort sind unter anderen die Paragraphen §§ 106 ff. zu betrachten.

Im Bereich des Zivilrechtes ist das Bürgerliche Gesetzbuch (BGB) mit zahlreichen Regelungen vertreten.

Im Gesetz gegen den unlauteren Wettbewerb (UWG) sind Regelungen betreffend unzumutbarer Werbung z.B. durch Telefon oder auch E-Mail zu finden (§ 7 Abs. 2 und 3 UWG), die nicht nur sogenannte Spamversender betreffen.

Im Strafrecht, also im Strafgesetzbuch (StGB), finden sich die wesentlichen Regelungen, die Störungen in der Datenverarbeitung unter Strafe stellen. Dazu gehören die Paragraphen § 202a StGB »Ausspähen von Daten« und § 263a StGB »Computerbetrug«. Der »Hackerparagraf« § 202c StGB beschreibt den Straftatbestand von Herstellung, Verkauf, Überlassung, Verbreitung oder Zugänglichmachung von Passwörtern oder Programmen für den Datenzugang. Dieser Tatbestand kann abhängig vom Unternehmenszweck für interne Prozesse relevant werden.

Noch zu erwähnen sind die klassischen Paragraphen § 303a StGB zum Straftatbestand der Datenmanipulation und der § 303b zur Computersabotage.

Firmen, die SOX oder Euro-SOX unterworfen sind, müssen aufgrund der darin unter anderem geforderten lückenlosen Protokollierung von Änderungen bereits entsprechende technische und organisatorische Vorkehrungen treffen.

Neben den erwähnten Gesetzen ist zu beachten, dass Stand heute jedes Land der Welt seine eigene Gesetzgebung im Bereich der IT-Security auf den Weg gebracht oder bereits in Kraft gesetzt hat. Viele Gesetze lesen sich dabei wie leicht modifizierte Kopien europäischer oder US-amerikanischer Gesetzes- texten und andere gehen in eine völlig andere Richtung. Zusätzlich dazu ist zu erwähnen, dass es ein Wettbewerbsvorteil für eine Region oder ein Land sein kann, die strengsten Gesetze zu etablieren und damit Unternehmen anzuziehen, die z.B. in großem Stil personenbezogene Daten verarbeiten. Insbesondere im Bereich des Datenschutzes ist hier ein Wettbewerb zu beobachten, der dazu führen könnte, dass die EU-Datenschutz-Grundverordnung nicht dauerhaft das umfassendste und weitreichendste Gesetz mit diesem Fokus



bleibt. Zu nennen ist hier beispielhaft der Katalog an Gesetzen rund um das Chinese Cyber Security Law.

3.4.4 Branchenstandards am Beispiel TISAX

Es ist seit Langem üblich, dass sich beispielsweise Automobilhersteller mit selbst entwickelten Fragekatalogen an ihre Lieferanten wenden, um den Stand der dort etablierten Sicherheitsmaßnahmen abzufragen. Teilweise haben sich daraus eigene, konzernweite Standards entwickelt, die sich ganz erheblich von Hersteller zu Hersteller unterscheiden. Diese unterschiedlichen Ansätze weichen nun zunehmend der Prüfung eines funktionierenden Managementsystems der Informationssicherheit auf Basis der Normen ISO 27001 und ISO 27002. Das bedeutet jedoch nicht, dass die Prüfkataloge nicht unterschiedliche Schwerpunkte setzen oder durch Aspekte weiterer Standards ergänzt werden können.

Es hat gleich mehrere Vorteile, ein gemeinsames Auditverfahren zu nutzen. So kann man sich zum einen auf eine Norm berufen, die selbst von staatlicher Seite aus anerkannt wird. Zum anderen wird die Vergleichbarkeit zwischen den Prüfungsergebnissen, die von unterschiedlichen Prüfern verschiedener Unternehmen ermittelt wurden, erleichtert. Die Zeiten, in denen zwei unterschiedliche Kunden beim gleichen Lieferanten infolge von Audits zu völlig verschiedenen Ergebnissen gekommen sind, sollen mit der Einführung von branchenweit normierten Audit-Prozessen der Vergangenheit angehören. Möchte man diese positiven Ergebnisse maximieren, erfordert dies den Einsatz des gleichen Fragenkatalogs als Basis, gleiche Regeln für alle Prüfdienstleister und die Überwachung durch eine unabhängige Instanz.

Neben den oben erwähnten Standards haben auch der Gesetzgeber und die Bundesbehörden wie das BSI einen Einfluss auf den Inhalt und die Schwerpunkte von Sicherheitsaudits. Ein wichtiges Gesetz in diesem Zusammenhang ist das IT-Sicherheitsgesetz (IT-SiG, siehe auch Abschnitt 3.4.2), das sich u.a. auf Unternehmen fokussiert, die als kritische Infrastrukturen identifiziert werden. Gemeinsam ist diesen Unternehmen, dass sie als wichtig für das Gemeinwesen gelten. In den Entwürfen für das IT-SiG 2.0 werden darüber hinaus Unternehmen mit großer Bedeutung aus wirtschaftlicher Sicht inkludiert, was den Kreis der betroffenen Unternehmen stark ausweiten wird. Aus den Vorgaben dieses Gesetzes wiederum haben Krankenhäuser, Energieversorger oder auch Wasserwerke eigene Sicherheitsstandards entwickelt, die



KAPITEL 3 – IT-COMPLIANCE

auf ihre Prozesse und zu schützenden Assets zugeschnitten sind. Unternehmen mit großer wirtschaftlicher Bedeutung müssen sich nun auch darauf vorbereiten, die Anforderungen des IT-SiG umzusetzen.

Ein weiterer wichtiger Schrittmacher für gemeinsame Auditstandards sind Verbände und Interessengemeinschaften. So schlagen Sicherheitsstandards wie TISAX (Trusted Information Security Assessment Exchange) des VDA (Verband der Automobilindustrie) oder TPISR (Third-Party Information Security Requirements) der AIAG (Automotive Industry Action Group) Wellen, da sie Vorgaben definieren, die weltweit viele Tausend Unternehmen direkt betreffen. Nämlich all diejenigen, die als Zulieferer für Verbandsmitglieder tätig sind. Untersuchungen zufolge, die der VDA durchgeführt hat, kann ein Unternehmen, das die Vorgaben aus TISAX einhält, damit rechnen, mit wenig Zusatzaufwand auch in einer TPISR-Überprüfung zu bestehen. Das liegt vor allem darin begründet, dass beide Anforderungskataloge auf der ISO-2700x-Reihe basieren, im Falle von TPISR angereichert durch technische Vorgaben aus den Standards des National Institute of Standards and Technology (NIST).

3

Wichtig

Nicht nur Audits auf Basis der Standards TISAX oder TPISR in der Automobilbranche, sondern auch Audits im Bereich der Energieversorger oder anderer kritischer Infrastrukturen richten ihr Augenmerk vermehrt auf die Informationssicherheit. Die Audit-Prozesse sind dabei immer ähnlich, wenn auch noch sehr stark unterschiedlich ausdetailliert. Die nachfolgend beschriebene Vorgehensweise kann damit immer häufiger auf andere Prüfstandards übertragen werden.

Die nachfolgenden Abschnitte werden sich mit dem Thema TISAX-Audit aus Sicht des IT-Security-Managers beschäftigen.

Vor dem Eintauchen in die Praxis empfehle ich dringend, eine Reihe von Standarddokumenten durchzuarbeiten, die der VDA und ENX auf ihrer Homepage zum Download anbieten. Alle Dokumente stehen standardmäßig in deutscher und englischer Sprache zur Verfügung. Die folgende Tabelle listet die wichtigsten davon.



Dokument	Kurzbeschreibung
Grundsätzliche Informationen	ENX-Website unter enx.com VDA-Website unter vda.de
VDA Information Security Assessment	VDA-Website Der Kern eines TISAX-Audits ist der ISA-Fragenkatalog in Excel-Form. »ISA« steht dabei für »Information Security Assessment«. Er beinhaltet neben den Fragen auch die Anforderungen an die jeweilige Umsetzung und eine Reihe von Erläuterungen.
TISAX-Teilnehmerhandbuch	ENX-Website Das Teilnehmerhandbuch ist die Betriebsanleitung für den kompletten Audit-Prozess.
Harmonisierung der Klassifizierungsstufen	VDA-Website Dieses Dokument beschreibt, wie die Klassifizierung von Informationen aufgebaut sein kann. Es ist ratsam, diesen Empfehlungen zu folgen und z.B. ein vierstufiges System aufzubauen, da es später die Kommunikation mit Kunden und anderen Lieferanten, die es ähnlich machen, erleichtert.
<Weitere Whitepapers des VDA>	VDA-Website Über die nächsten Jahre sollen eine Reihe von Whitepapers veröffentlicht werden, die als Hilfestellung zur Implementierung eines ISMS nach TISAX gedacht sind. Es lohnt sich, regelmäßig zu überprüfen, ob weitere Dokumente verfügbar sind.

3

Die Hauptakteure, die hinter TISAX stehen, sind die großen Automobilhersteller in Deutschland in engem Informationsaustausch mit staatlichen Stellen. Folgende Aspekte spielen bei der Entwicklung eine maßgebliche Rolle:

- Die Verantwortung für die Erfüllung von z.B. gesetzlichen Regeln wie dem IT-SiG oder der EU-Datenschutzgrundverordnung werden bei TISAX vom Gesetzgeber über den Hersteller an die Zulieferer weitergereicht. Daraus ergeben sich eine Reihe von Vorteilen für die Hersteller, da sie damit ihre Verpflichtung zur Sicherstellung von Datensicherheit und Datenschutz entlang der Lieferkette gewährleisten können.



- Durch die Umsetzung der Vorgaben werden in sehr kurzer Zeit sehr viele Unternehmen auf ein akzeptables Sicherheitsniveau gehoben. Dass der Druck der Hersteller auf die Zulieferer dabei eine große Rolle spielt, ist hier Mittel zum Zweck. Das ist auch die Perspektive der Bundesregierung und damit des BSI, wenn sie den Kontakt zu den Verbänden suchen. Kaum ein anderes Vorgehen hat in diesem Umfang so positive Auswirkungen auf die Unternehmenssicherheit in einer ganzen Branche bewirkt. Die schieren Zahlen belegen dies. So haben bereits mehrere Tausend Audits stattgefunden, die mehrere Zehntausend Abweichungen aufgedeckt haben, die bereits heute, mit einem Aufwand, geschlossen wurden.
- Für den Lieferanten ergibt sich die Chance, ein solches Audit einmalig zu absolvieren und sicher sein zu können, dass das Testat bei allen im VDA organisierten Unternehmen anerkannt wird. Das Testat behält für drei Jahre seine Gültigkeit.

Die Hauptmotivation für den Hersteller wie für den Lieferanten sollte aber in jedem Fall sein, das eigene und das ihm von den Kunden anvertraute Know-how zu schützen und damit die eigene Wettbewerbsfähigkeit zu erhöhen.

3.4.5 ISO 27001 und TISAX

Die Erfahrung zeigt, dass eine erfolgreiche Zertifizierung nach ISO 27001 nicht automatisch auch bedeutet, sich für ein TISAX-Label zu qualifizieren. Diese Erkenntnis ist für viele Unternehmen zunächst überraschend, ist aber nur folgerichtig, wenn man die Ziele der ISO 27001 und die von TISAX miteinander vergleicht. TISAX ist nicht angetreten, um einen allgemeingültigen Sicherheitsstandard für alle Unternehmensgrößen und Branchen auf Basis von unternehmerischem Risikomanagement zu entwickeln. Es geht hier vielmehr um konkretere Ziele, nämlich darum, die Implementierung eines vergleichbaren Sicherheitsstandards in allen Unternehmen der Automobilzulieferindustrie zu forcieren. Abweichungen in der Art der Umsetzung des gewünschten Sicherheitsniveaus werden deshalb effektiv vermieden, indem nicht nur vorgegeben wird, **was** zu tun ist, sondern auch, **wie** dies zu geschehen hat. Mit diesen detaillierteren Vorgaben werden im Rahmen des Risikomanagements die Auswahlmöglichkeiten bei der Risikobehandlung effektiv um die Wahlmöglichkeit »Tragen des Risikos« reduziert. Das ist beachtenswert, denn es wirkt sich direkt auf den Risikomanagementprozess der auditierten Firma aus und verkleinert den Rahmen der unternehmerischen Freiheit.



im Umfeld der Informationssicherheit. Das betrifft auf den ersten Blick nur die Daten des Auftraggebers. Weil diese aber häufig nicht von den eigenen Daten zu trennen sind, da sie die gleiche Infrastruktur benutzen, erweitern sich die darauf gemünzten Regeln automatisch auch auf die eigenen Assets.

Ein weiterer wichtiger Unterschied ist, dass es im Rahmen von TISAX nicht möglich ist, im Statement of Applicability (SoA) einzelne Controls auszuschließen, falls diese aus Sicht des Auftraggebers erforderlich sind und sie – wenn auch nur theoretisch – die Verarbeitung von Kundendaten beinhalten. Anders ausgedrückt: Controls können nur dann von der Prüfung ausgenommen werden, wenn dargestellt werden kann, dass keine Kundendaten betroffen sind.

Nach annähernd 50 TISAX-Audits, die ich selbst begleitet habe, durchgeführt von einer ganzen Reihe verschiedener Prüfdienstleister, kann ich mehrere Dinge aus eigener Erfahrung konstatieren:

- TISAX-Audits sind stringenter und gleichförmiger als Audits vergleichbarer Art, die sich jedes Mal, trotz ähnlichem oder sogar gleichem Auditkatalog, signifikant voneinander unterscheiden. Damit ist auch die Vergleichbarkeit zwischen den Ergebnissen besser. Dies wird u.a. durch intensive Schulungen der Prüfdienstleister erreicht.
- Auch wenn TISAX-Audits standardisierter sind und die Prüfdienstleister ein vergleichbares Vorgehen einüben, spielen dennoch Kriterien wie die Expertise des Prüfers, das Land, in dem das Audit durchgeführt wird, und die Art der Vorbereitung weiterhin eine gewisse Rolle. Es lohnt sich also auch hier, zunächst zu prüfen, ob die Chemie zwischen dem Prüfer und dem eigenen TISAX-Team stimmt.
- Eine ISO-27001-Zertifizierung erreicht zu haben, ist hilfreich, aber nicht ausreichend, um auch ein TISAX-Testat zu erhalten.
- Jede Frage des Prüfers erfordert dreierlei Antworten:
 - Den Nachweis, dass eine diesbezügliche Regelung existiert und bei den betroffenen Personen bekannt ist
 - Die Darstellung, dass der mit der Regelung verbundene Prozess das Risiko akzeptabel reduziert
 - Das Aufzeigen eines kompletten Prozessbeispiels mit Nachweisen
- Eine gute Vorbereitung, das richtige Team, die richtige Einstellung und das Vermeiden von Grundsatzdiskussionen über den Sinn und Zweck ein-



zerner Maßnahmen sind der Schlüssel für einen positiven Bescheid. Es gilt, mit dem Prüfdienstleister zu kooperieren, anstatt mit ihm zu disputeren. Dafür sind die Vorgaben vonseiten des ENX und des VDA zu stark ausdefiniert.

- Jede Frage im Audit steht in direktem Zusammenhang mit einem oder mehreren Controls und den darin enthaltenen Unterpunkten. In den meisten Controls sind die Vorgaben nicht so ausdetailliert, als dass sich nicht mehrere Möglichkeiten ergeben würden, um die jeweilige Vorgabe zu erfüllen. Es kommt immer darauf an, den Prüfer davon zu überzeugen, dass die eingesetzten Maßnahmen das Risiko in ausreichendem Maße reduzieren.

3.4.6 Vorbereitende Maßnahmen

3

Beteiligte Parteien

Die wichtigsten Partner in einem TISAX-Audit sind der Auftraggeber, derjenige, der einer Prüfung unterzogen wird, und der Prüfdienstleister. Der Auftraggeber definiert das Prüfziel und damit die grundlegenden Parameter einer Prüfung. Das Prüfziel wiederum orientiert sich am Schutzbedarf der verarbeiteten Kundendaten. Abhängig vom Prüfziel wird das Audit vorwiegend telefonisch auf Basis von ausgetauschten Nachweisen stattfinden oder aber vor Ort durch den Prüfdienstleister. Dem geprüften Unternehmen steht es frei, das Prüfziel zu erhöhen, um sicherzustellen, dass das Testat in jedem Fall auch späteren, erhöhten Kundenanforderungen genügt. Fordert der Kunde z.B. eine Prüfung auf Basis »Informationen mit hohem Schutzbedarf«, dann kann es für ein Unternehmen durchaus Sinn machen, eine Prüfung auf Basis »Informationen mit sehr hohem Schutzbedarf« durchführen zu lassen für den Fall, dass ein zweiter Kunde genau dies einfordern könnte.

Wichtig

Das Heranziehen von Kollegen aus verschiedenen Unternehmensbereichen, unter Umständen auch die Beauftragung externer Spezialisten und nicht zuletzt die Umsetzung von Maßnahmen auf Basis von identifizierten Abweichungen verursachen oft nicht unerhebliche Kosten. Deshalb sind die frühzeitige Einbindung und die vorbehaltlose Unterstützung der Unternehmensleitung entscheidend für den Erfolg.



Weitere Faktoren, die den Aufwand bestimmen, sind

- die eigene Unternehmensgröße,
- der Stand der Informationssicherheit
- und die Qualifikation der eigenen Mitarbeiter.

Naturgemäß variieren diese Parameter sehr stark von Unternehmen zu Unternehmen.

Innerhalb des eigenen Unternehmens tragen die Fachbereiche

- Informationssicherheit,
- IT-Security, IT,
- Personalabteilung,
- Entwicklungsabteilung,
- Datenschutz,
- Einkauf
- und die Rechtsabteilung

– mehr oder weniger in dieser Reihenfolge – die Hauptlast eines Audits. Dazu kommt diejenige Organisation, die die TISAX-Audits koordiniert, den Prüfdienstleister aussucht, Termine vereinbart, unter Umständen Schulungen vermittelt oder sogar selbst durchführt und letzten Endes übergreifend die Behebung der Haupt- und Nebenabweichungen einfordert und nachverfolgt.

Datenaustausch mit dem Prüfdienstleister

Neben der Einarbeitung der eben aufgeführten Experten gilt es, die technischen Grundlagen für die Kommunikation zwischen den beteiligten Parteien zu schaffen. Da der Auditor mit der Sichtung bestehender Nachweise, wie z.B. Richtlinien, bereits im Vorfeld einer Prüfung oder eines Pre-Audits beginnen wird, muss ein sicherer Weg des Datenaustauschs gefunden werden. Dieser dient dann der sicheren Übermittlung von Dokumenten. Auch hier gilt, dass den internen Regelungen zum Dokumentenaustausch Folge geleistet werden sollte. Sind Dokumente als »Streng geheim« klassifiziert, ist es vermutlich nicht erlaubt, diese mit Dritten, also den Prüfern, zu teilen. Dem ersten Impuls, dem Prüfer alles zu schicken, was man hat, und ihn dann selbst nach den wesentlichen Punkten suchen zu lassen, ist dabei schlechter Stil und



führt häufig genug zu Missverständnissen. Im Grunde muss man einen Kompromiss finden, der im besten Fall die Zuordnung von Controls zu den einzelnen Dokumenten oder gar Kapiteln innerhalb von Dokumenten beinhaltet.

Durchführung von Pre-Audits

Die Durchführung sogenannter Pre-Audits, am besten zusammen mit dem Prüfdienstleister, der später auch die Audits durchführen wird, dient der ersten Ermittlung von Abweichungen, ohne dass man dabei bereits an die Regeln, die zeitlichen Vorgaben oder die Herangehensweise eines TISAX-Audits gebunden ist. Regelmäßig dauern Pre-Audits zwei oder mehr Tage, in denen es durchaus vorkommen kann, dass man sich bis zu zwei Dritteln der Zeit auf IT-Themen konzentriert. Diese intensive Darstellung der eigenen Umgebung und der eingeführten Sicherheitsmaßnahmen ist bei einem regulär durchgeführten Audit aufgrund des Zeitdrucks häufig nicht in diesem Umfang möglich.

3

Wichtig:

Ein Prüfdienstleister, der ein TISAX-Audit durchführen wird, darf nicht im Vorfeld als beratende Instanz auftreten. Dies wäre ein Interessenkonflikt. Ein Pre-Audit ist deshalb keine Beratungsleistung, sondern ein sogenanntes »better practice« und damit eher ein Gespräch, zu dem der Prüfdienstleiter mit Hilfestellungen beiträgt – gemäß dem Motto: »Was würde ich persönlich besser machen?«

Die eben geschilderten Rahmenbedingungen haben zur Folge, dass es kein Standardvorgehen bei der Durchführung von Pre-Audits gibt. Da man sich als Geprüfter aber wünscht, möglichst per Control Verbesserungspotenzial oder gar Abweichungen gemeldet zu bekommen, gehen viele Prüfdienstleister auf Basis des Prüfkatalogs vor und bereiten die Ergebnisse auch dementsprechend auf.

Ein weiterer Vorteil ist der, dass zwischen einem Pre-Audit, das vielleicht große Abweichungen im Bericht auflistet, und dem TISAX-Audit eine beliebige Zeitspanne vergehen kann. Erst mit dem Start des TISAX-Audits beginnen die üblichen Fristen.



3.4.7 Fragenkatalog

Der TISAX-ISA-Fragenkatalog orientiert sich stark an der ISO-27002-Norm – sowohl was die Gliederung angeht als auch bei der Auflistung der Maßnahmen. Während in der Norm aber mögliche Maßnahmen nur gelistet werden, definiert TISAX auch deren Ausprägung. Dies erfolgt in Form von Stichworten, deren genaue Einordnung den Prüfdienstleitern in Schulungen nähergebracht wird. Die auditierte Firma, die ohne dieses Vorwissen nur den Fragenkatalog kennt, muss sich selbst erarbeiten, inwieweit den Anforderungen adäquat entsprochen werden kann. Die wichtigste Frage, die sich dabei stellt, lautet: »Was muss ich mindestens tun, um das Audit zu bestehen?« Dieser Abschnitt soll darauf eine erste Antwort liefern.

Der Fragenkatalog, den die meisten Prüfdienstleister konsequent seriell abarbeiten, beinhaltet einige Punkte, die wiederholt auftreten und die sich deshalb auch von vornherein zusammenfassen lassen. Dazu gehören vor allem die folgenden:

Cloud Computing: In mehreren Controls wird auf die Nutzung von Cloud-Dienstleistern eingegangen. Das reicht von der technischen Infrastruktur über die Möglichkeit, Daten in das Unternehmen zurückzuholen, bis hin zum Einkaufsprozess. Falls Richtlinien und Nachweise vorliegen, die alle diese Punkte bereits beantworten, kann dies oft in einem Rutsch abgearbeitet werden.

Verschlüsselung: Ähnlich wie im Thema Cloud Computing verhält es sich auch bezüglich der Verschlüsselung von Daten. Dazu gibt es Vorgaben in mehreren Controls, die praktischerweise zusammengefasst werden sollten.

Wichtig:

Aktuell befinden wir uns im Übergang von Version 4 auf Version 5 des TISAX-ISA-Fragenkatalogs. Die nachfolgende Tabelle orientiert sich primär an der neuen Version 5, deckt aber auch die Version 4 ab.

Jede Anforderung im TISAX-ISA-Fragenkatalog beinhaltet immer auch eine Liste der erforderlichen Teilmaßnahmen. Die nachfolgende Tabelle liefert zusätzliche Informationen und Hintergrundinformationen und führt die Punkte aus dem Fragenkatalog nicht erneut auf.



KAPITEL 3 – IT-COMPLIANCE

In einem ersten Schritt ist es erforderlich, die aktuelle Version des TISAX-ISA-Fragenkatalogs von der Webseite des VDA herunterzuladen. Es macht Sinn, den Fragenkatalog und die darin enthaltenen Vorgaben parallel zu den Hilfestellungen in der nachfolgenden Tabelle zu lesen. Einen Bezug zwischen Control und Hilfestellung herzustellen, ist nicht direkt möglich, da verschiedene Versionen des TISAX-ISA-Fragenkatalogs im Umlauf sind und sich die Inhalte voneinander unterscheiden. Aus diesem Grund werden in der ersten Spalte inhaltliche Stichworte aufgeführt, die helfen sollen, den Bezug zu den Maßnahmen im Fragenkatalog herzustellen.

Stichworte zum Thema	Hilfestellung
<p>Information-Security-Management-System (ISMS)</p> <p>Organisation der Informationssicherheit</p> <p>Verantwortlichkeiten in der IT-Security-Organisation</p> <p>IS-Politik (Sicherheitsrichtlinie), die in Abschnitt 5.2 der ISO 27001 näher spezifiziert wird</p>	<p>Die Sicherstellung von Vertraulichkeit, Verfügbarkeit und Integrität der im Geltungsbereich des Audits befindlichen (Kunden-)Daten durch den Betrieb eines organisierten und umfassenden Sicherheitsmanagements ist die Kernanforderung der ersten Fragen im Fragenkatalog. Diese Anforderung ist die wichtigste Anforderung und zu Beginn des Audits auch diejenige, deren Beantwortung die Weichen für das gesamte Audit stellt.</p> <p>Die Beantwortung dieser Frage beginnt deshalb am besten mit der Vorlage der IS-Politik, unterschrieben von der Unternehmensleitung. Darin wiederum werden einige Teilfragen des ersten Punktes beantwortet. Dazu gehören Fragen nach der Angemessenheit der definierten Prozesse, die Definition von Verantwortlichkeiten und die Festlegung des Geltungsbereichs. Die Ausprägung dieser verschiedenen Punkte muss zum Schutzbedarf der Kundendaten, um die es ja geht, passen und der Geltungsbereich des ISMS muss diese miteinschließen.</p> <p>Das Organigramm der Security-Organisationen ist ein wichtiger Gradmesser für die Wichtigkeit, die dem Informationsschutz im Unternehmen eingeräumt wird. An dieser Stelle ist es hilfreich, wenn das Organigramm die Unabhängigkeit und die Weisungsbefugnisse des IT-Security-Managers widerspiegelt. Im Rahmen der ISMS-Prozesse gilt das Gleiche: Die Verantwortlichkeiten müssen geregelt und die Wirksamkeit dieser Regelungen nachweisbar sein.</p>



Stichworte zum Thema	Hilfestellung
	<p>Die Organisation der Security im Unternehmen, heruntergebrochen von den Aufgaben der Unternehmensleitung über die Hauptniederlassungen bis hin zu den einzelnen Standorten, ist an diesem Punkt darzustellen. Vorzugsweise stellt der lokal zuständige Sicherheitsverantwortliche diesen Zusammenhang persönlich vor und macht damit deutlich, dass keine Bereiche existieren, für die es, aus Sicht der Security, keinen Zuständigen gibt.</p> <p>Die Qualifikation der Mitarbeiter der Sicherheitsorganisation ist ein Punkt auf der Liste der Auditoren und kann mittels absolviert Schulungen und Zertifikate aufgezeigt werden.</p> <p>Da die meisten Sicherheitsvorgaben üblicherweise in der Unternehmenszentrale festgelegt werden und deshalb auch die meisten Mitarbeiter der Sicherheitsorganisation dort angesiedelt sind, ist es immer eine Herausforderung, die dort aufgestellten Regeln und die daraus abgeleiteten Maßnahmen bis in die lokale Organisation zu transportieren. Ein weiterer wichtiger Punkt ist die Art der Kommunikationsmittel, die dazu eingesetzt werden, alle Betroffenen zu informieren, zu schulen und anzuweisen. Dies bezieht sich im Rahmen des TISAX-Audits vor allem auf die Bereiche Unternehmensleitung, Informationstechnologie, Personalabteilung, Einkauf, Entwicklung, Vertrieb und alle Externen, die für diese Bereiche tätig werden. Während des initialen Rundgangs durch den Standort sollte deshalb z.B. auf diesbezügliche Aushänge, Hinweisschilder, Regelwerke für Externe oder Flyer hingewiesen werden.</p> <p>Im Rahmen des Plan-Do-Check-Act-Zyklus wird auch das ISMS stetig weiterentwickelt und verbessert. Zu diesem Zweck werden die verschiedenen Richtlinien überprüft und angepasst und die Sicherheitsprozesse verbessert. Diesen Kontroll- und Verbesserungszyklus darzustellen, rundet die Erläuterung des ISMS ab.</p>



Stichworte zum Thema	Hilfestellung
IT-Security Policies	<p>Neben der IS-Politik werden auch das Vorhandensein und die Qualität aller weiteren Richtlinien geprüft, die die verschiedenen Vorgaben der ISO 27002 und des Fragenkatalogs beinhalten. Eine dokumentierte Richtlinienstruktur wird dabei als Grundlage der Diskussion vorausgesetzt.</p> <p>Die Prüfdienstleister investieren einen Großteil ihrer Arbeitszeit in das Studium der einzelnen Richtlinien und überprüfen dann im Weiteren deren Umsetzung. Dies beinhaltet alle Richtlinien, angefangen bei der sogenannten IS-Politik bis hin zu den typischen Richtlinien im Security-Umfeld.</p> <p>Der Life-Cycle jeder Richtlinie muss einer Reihe an Anforderungen genügen:</p> <ul style="list-style-type: none">■ Jede Richtlinie muss von der zuständigen Stelle freigegeben worden sein.■ Jede Anforderung, die im Fragenkatalog aufgeführt ist, muss eine Entsprechung in einer Richtlinie des Unternehmens haben,■ sie muss regelmäßig überprüft werden,■ alle Betroffenen müssen sie kennen,■ sie muss technisch in einer Art und Weise zur Verfügung gestellt werden, die einen unkomplizierten Zugriff ermöglicht,■ die Verbindlichkeit muss klar herausgestellt werden und■ für die Nichtbeachtung müssen Konsequenzen festgelegt sein. <p>Die Arbeitsverträge, zumindest der Personen, die mit Kundendaten umgehen, sollten die Verpflichtung zur Einhaltung von Unternehmensrichtlinien beinhalten. Auch Aushänge oder regelmäßige Kommunikation per E-Mail oder Intranet sind gute Hinweise für ein funktionierendes Richtlinienmanagement.</p>
Sicherheitsaspekte in Projekten	Die Richtlinie zur Durchführung von Projekten oder zumindest das Projekthandbuch muss den Aspekt Security beinhalten.



Stichworte zum Thema	Hilfestellung
	<p>Dies beginnt bei der Klassifizierung der im Projekt, und nachher im Betrieb, verarbeiteten Daten. Handelt es sich um ein Kundenprojekt, sollte die Beschreibung, wie die Klassifizierung vorzunehmen ist, den Weg von der Kundeneinstufung hin zur eigenen Einstufung des Projekts beinhalten. Dies fällt umso leichter, wenn die Anzahl der Schutzstufen und deren Bedeutung mit den Einstufungen des Kunden harmonieren.</p> <p>Wird eine Software genutzt, um Projekte zu verwalten, dann ist es hilfreich, wenn diese die Klassifizierung jedes Projekts darstellen kann.</p> <p>Anhand der Einklassifizierung des Projekts müssen entsprechende Maßnahmen abgeleitet werden, die im Projektlauf Beachtung finden müssen. Dazu kann z.B. der Umgang mit Projektdaten des Kunden oder die Behandlung von Prototypen gehören.</p>
Sicherheitsaspekte im Zusammenhang mit externen Diensteanbietern und Diensten (z.B. Cloud-Diensten)	<p>Analog zum Assetmanagement müssen auch die externen Dienstleistungen, die das Unternehmen in Anspruch nimmt, zunächst identifiziert und im Rahmen eines Assetmanagements verwaltet werden.</p> <p>Handelt es sich zudem um die Verarbeitung von Daten bei externen Dienstleistern (Cloud-Dienste), muss die Prüfung, ob dies gestattet ist, im Vorfeld auf verschiedenen Ebenen vollzogen worden sein. Diese beinhalten die Überprüfung der Einhaltung von IT-Security-Richtlinien und den Vorgaben des Datenschutzes. Der Prozess der Prüfung sollte in einer gesonderten Richtlinie festgehalten werden.</p> <p>Die Prüfung von Diensteanbietern auf die Einhaltung von Richtlinien ist nur bedingt möglich. Das liegt daran, dass es kaum möglich ist, die Infrastruktur und die Prozesse eines Dritten in der erforderlichen Tiefe zu prüfen. Dennoch sollten Anforderungen an Diensteanbieter schriftlich in einer Richtlinie festgehalten werden und die Einhaltung dieser Vorschriften von den externen Unternehmen schriftlich bestätigt werden.</p>



Stichworte zum Thema	Hilfestellung
Assetmanagement	<p>Das Register der Assets ist immer der Ausgangspunkt für die Überprüfung des Assetmanagements und später auch des Risikomanagements. Assets, das können z.B. IT-Systeme sein, aber auch Personen, Prototypen, Räumlichkeiten oder Daten. In besonderem Maße wird im Rahmen des TISAX-Audits auf diejenigen Assets geschaut, die Eigentum desjenigen sind, der das Audit beauftragt hat: des Kunden. Da es im Zweifelsfall aber schwerfallen wird, genau zu trennen, wo die eigenen Daten enden und die des Kunden beginnen, ist es angebracht, alle Assets zu erfassen und zu inventarisieren.</p> <p>Das Assetmanagement beinhaltet viel mehr als nur die Liste der Assets. Das Management der Assets spannt vielmehr den Bogen von deren Klassifizierung über die Risikobewertung bis hin zur Ableitung von Maßnahmen. Einen solchen Eintrag kann man sich also als Zusammenführen von verschiedenen Informationen aus verschiedenen Bereichen des IT-Sicherheitsmanagements vorstellen.</p> <p>Ein Beispiel:</p>
ServerA.kiel.unternehmen.de	Datenserver mit Freigaben für Projektdaten
Vertraulichkeit	Streng vertraulich
Anforderungen an die Verfügbarkeit	Maximale Downtime von 4 Stunden
Anforderungen an die Integrität	Hoch
Link zum Notfallplan	X:\Notfallplaene\Server RZ Kiel\datenserver.pdf
Bedrohungen	Diebstahl, Ungenehmigter Zugriff, Datenverlust
Maßnahmen	Aufstellort: Rechenzentrum Kiel Verschlüsselung der Daten, Zugriffskonzept, Sicherungskonzept
Link zu den Maßnahmen-dokumenten	X:\Maßnahmen Kiel\...



Stichworte zum Thema	Hilfestellung
	Natürlich macht es Sinn, die verschiedenen Asset-Typen zu clustern. So kann man leicht alle Datenserver mit den gleichen Attributen zusammenfassen. Noch leichter fällt dies bei sehr stark standardisierten Assets wie Mobiltelefonen oder Laptops von Benutzern.
Klassifizierung und Management von Assets	An dieser Stelle wird der Vorgang der Klassifizierung von Assets mit dem Management von Assets zusammengebracht. Im Rahmen des Assetmanagements werden Assets, bzw. Kategorien von Assets, aufgeführt und mit einer Einklassifizierung nach Vertraulichkeit, Verfügbarkeit und Integrität versehen. Abhängig von der jeweiligen Klassifizierung werden aus einem Maßnahmenkatalog die adäquaten Schutzmaßnahmen ausgewählt und zugewiesen. Um die Sichtbarkeit der jeweilig zugewiesenen Klassifizierung zu gewährleisten, werden die einzelnen Assets zudem beschriftet. Bei Dokumenten wird diese Beschriftung im Allgemeinen sichtbar im unteren Bereich hinzugefügt, während sie z.B. bei Räumlichkeiten in Form von Markierungen an den Türen geschehen kann.
Risikomanagement der Informationssicherheit	Der Risikomanagementprozess muss genauso geregelt sein wie andere Sicherheitsprozesse auch. Dies beinhaltet <ul style="list-style-type: none">■ einen entsprechenden Verweis in der Sicherheitsrichtlinie (IS Policy),■ eine explizite Richtlinie, die den Umfang und den Prozess zum Risikomanagement festlegt,■ sowie Verantwortlichkeiten und Kompetenzen. Auf Basis dieser Dokumente und einiger Stichproben wird im Laufe des Audits überprüft, wie das Unternehmen auf eine bestimmte Risikoeinschätzung gekommen ist und wie die daraus abgeleiteten Maßnahmen verfolgt und umgesetzt wurden. Das Assetmanagement stellt auch hier den Dreh- und Angelpunkt dar. So ist es z.B. sinnvoll, einen Eintrag, der »Mobiltelefone« heißt, direkt mit der Risikoeinschätzung für diese Kategorie von Assets und die daraus abgeleiteten Maßnahmen zu verknüpfen.



Stichworte zum Thema	Hilfestellung
	<p>Die Effektivität des Risikomanagement-Prozesses steht hierbei im Vordergrund. Das bedeutet aber nicht, dass der Zusammenhang zwischen Asset, Bedrohungen, Schwachstellen, Risikoeinschätzung und Maßnahmen nicht vollständig dargestellt werden muss.</p> <p>Es hat sich bewährt, einen anerkannten Bedrohungskatalog wie den des BS, als Grundlage für einen eigenen Bedrohungskatalog zu nutzen.</p>
Überprüfung der Wirksamkeit des ISMS (durch eine unabhängige Stelle)	<p>Die Wirksamkeit des ISMS als Ganzes sicherzustellen, ist Aufgabe der Unternehmensleitung. Diese wiederum ist darauf angewiesen, dass entsprechende Stellen sie dahin gehend beraten. Je unabhängiger diese beratenden Stellen sind, desto höher wird die Qualität der Überprüfung eingeschätzt. Ideal ist deshalb die regelmäßige Überprüfung des ISMS durch eine externe Stelle. In den meisten Fällen wird es aber eine interne Stelle geben, die diese Aufgabe wahrt und die Ergebnisse regelmäßig an die Unternehmensleitung berichtet.</p> <p>Im Rahmen eines ISO-27001-Zertifizierungsprozesses würde die Überprüfung der ISMS-Prozesse ein wichtiges Testkriterium darstellen. Die TISAX-Methodik ist an dieser Stelle jedoch deutlich genügsamer. Vor einem TISAX-Audit lohnt sich ein Blick auf die beispielhaften Kennzahlen im Reiter »KPIs« des Fragenkatalogs. Auch wenn die dort aufgeführten Grenzen selbst für Prüfer zu unscharf sind, geben sie doch einen wichtigen Anhaltspunkt, was in einem TISAX-Audit bezüglich der Überprüfung des ISMS von Belang ist.</p> <p>Ein guter Weg ist hierbei, sich eine Reihe von Controls herauszusuchen und Kennzahlen zu ihnen zu entwickeln. So kann mit dem Control »Schutz vor Schadsoftware« eine ganze Reihe von Kennzahlen verbunden werden. Dies reicht von der Zeitspanne, innerhalb derer neue Antivirus-Patterns eingespielt werden, bis hin zur Reaktionszeit des PC-Supports, wenn auf einem Arbeitsplatzrechner ein neuer Trojaner entdeckt wird.</p>



Stichworte zum Thema	Hilfestellung
	Auch hier gilt die Devise, dass Kennzahlen, die automatisiert erfasst werden, die besseren Kennzahlen sind. Sofern ein Monitoring-System etabliert ist, sollte man also zunächst dort suchen, ob es nicht bereits geeignete Kennzahlen gibt, die auf Controls des Frankenkatalogs gemappt werden können.
Überprüfung der Einhaltung von Richtlinien und Sicherheitsverfahren	<p>Das Management von Sicherheit im Unternehmen wird maßgeblich über die Richtlinien gesteuert. Richtlinien beschreiben, wer was in welcher Reihenfolge zu tun hat, und stellen damit die Blaupause für alle Verfahren im Sicherheitsmanagement dar. Die Überprüfung der Einhaltung von Richtlinien ist wiederum die Aufgabe der Auditabteilung.</p> <p>An dieser Stelle ist aufzuzeigen, welche Arten von Auditverfahren innerhalb des Scopes zum Einsatz kommen. Ideal ist es, wenn die ganze Bandbreite an Methoden vorhanden ist. Diese würde von automatisierten Schwachstellenscans bis hin zu Vor-Ort-Audits reichen. In allen Fällen ist der Prozess bis hin zur kontrollierten Abarbeitung gefundener Abweichungen nachzuweisen.</p>
Informationssicherheitsereignisse (Security Incident Management)	<p>Das Erkennen, Melden und Verarbeiten von Sicherheitsereignissen ist ein wesentlicher Punkt des Business Continuity Managements. Dabei ist nicht jedes Sicherheitsereignis gleichzusetzen mit einem IT-Sicherheitsereignis. So ist das unbefugte Eindringen in ein Gebäude eher durch den Bereich Werkschutz zu behandeln, während das Auftreten von Schadsoftware in den Bereich der IT-Security fällt. Für beide Arten von Sicherheitsereignissen sind entsprechende Prozesse zu beschreiben und zu etablieren. Zumindest die folgenden Punkte müssen diesbezüglich nachgewiesen werden:</p> <ul style="list-style-type: none">■ eine entsprechende Richtlinie, die den Prozess und die Verantwortlichkeiten beschreibt■ Formulare oder eine entsprechende Software, die den Prozess unterstützt und der Dokumentation dient■ Stichproben von in der Vergangenheit behandelten Sicherheitsereignissen



Stichworte zum Thema	Hilfestellung
	Hat man den jeweiligen Prozess stark nach ISO 27035 ausgerichtet, genügt dies den Anforderungen von TISAX.
Verpflichtung der Mitarbeiter	<p>Jeder Mitarbeiter und jeder externe Dienstleister, der mit Kundendaten arbeitet, sollte zum einen eine Geheimhaltungsverpflichtung unterzeichnet haben und zum anderen eine Verpflichtung auf die Einhaltung der Sicherheitsrichtlinien. Am besten geschieht dies bei Mitarbeitern bereits im Rahmen des Arbeitsvertrags.</p> <p>An einer möglichst zentralen Stelle werden diese Schriftstücke verwaltet und können dem Auditor gezeigt werden.</p> <p>Zudem sollen die Voraussetzungen für die Einleitung personalrechtlicher Maßnahmen bei Verstößen geschaffen werden.</p>
Awareness-Maßnahmen und -Schulungen	<p>Schulungen, Plakataktionen, Gewinnspiele etc. sind alles Bausteine einer konzentrierten Schulungsmaßnahme im Bereich der IT-Security. An dieser Stelle ist die Strategie des Unternehmens aufzuzeigen.</p> <p>Um den Wirkungsgrad der Awareness-Maßnahmen zu messen, ist es wichtig, entsprechende Kennziffern zu erstellen. Dabei kann es sich z.B. um den prozentualen Anteil an erfolgreich durchgeführten Maßnahmen pro Lokation handeln.</p>
Sicherheitszonen	<p>Eine der wichtigsten Dokumentationen, die bei einem Audit vorgelegt werden müssen, ist ein Übersichtsplan über die Gebäude und Räumlichkeiten, die im Gelungsbereich liegen, ergänzt durch Kennzeichnungen der verschiedenen Sicherheitszonen. Die Kennzeichnungen müssen denen entsprechen, die in der dazugehörigen Sicherheitszonenrichtlinie definiert wurden.</p> <p>Anhand dieser Dokumentation wird die Sicherheitsbegutachtung stattfinden, die die Überprüfung der Zugangskontrollen beinhaltet.</p> <p>Die Maßnahmen, die auf Basis der jeweiligen Klassifizierung umgesetzt werden müssen, werden in der zugehörigen Sicherheitszonenrichtlinie beschrieben.</p>



Stichworte zum Thema	Hilfestellung
	<p>Übliche Maßnahmen sind z.B. Zutrittskontrollsysteme, das Abkleben von Fenstern, um die Einsicht in vertrauliche Bereiche zu verhindern, Schranken, Videoüberwachungssysteme, Zäune, ein zentraler Empfang, Ausweistragepflicht, Pläne zum Werksschutz, aber auch Regeln für den Umgang mit Log-Dateien, die den Zutritt von Personen aufzeichnen.</p> <p>Es ist wichtig, Gebäudepläne und Richtlinien für diesen Themenbereich aktuell zu halten.</p>
Business Continuity Management	<p>Das Schutzziel »Verfügbarkeit« wird weitgehend unter diesem Punkt zusammengefasst und fragt zum einen die lokationspezifischen Notfall- und Wiederanlaufpläne ab und zum anderen die typischen IT-Systeme wie Backup und Restore. Auch hier sind zunächst die entsprechenden Richtlinien zu zeigen. Anhand dieser Richtlinien und einiger Stichproben wird danach ermittelt, ob die beschriebenen Prozesse vollständig sind und eingehalten wurden.</p>
Mobile Endgeräte und Speicher	<p>Drei Arten von mobilen Endgeräten stehen im Fokus dieses Punktes. Dabei handelt es sich um Smartphones, Laptops und mobile Speicher wie USB-Sticks.</p> <p>Smartphones:</p> <p>Zwei Aspekte der Benutzung von Smartphones müssen durch Richtlinien geregelt werden – zum einen die technische Verwaltung und Konfiguration und zum anderen die Vorgaben für die Benutzer. Diese beiden Richtlinien werden häufig von verschiedenen Stellen veröffentlicht. Die erste Richtlinie deckt technische Aspekte ab und wird deshalb häufig in der Unternehmenszentrale von der IT veröffentlicht. Die Richtlinie bezüglich der Benutzeraspekte kommt hingegen meist eher aus der Personalabteilung und kann in verschiedenen Ländern aufgrund lokaler Gesetze unterschiedliche Ausprägungen haben.</p> <p>Im Rahmen des Audits wird Wert auf die Darstellung der lokalen Umsetzung dieser Richtlinien gelegt. Dies beinhaltet die Listung der Geräte im lokalen Assetmanagement genauso wie die technische Umsetzung der Vorgaben.</p>



Stichworte zum Thema	Hilfestellung
	<p>Laptops: Auch in Bezug auf Laptops wird zwischen den technischen Vorgaben, die maßgeblich die IT-Abteilung umsetzt, und den Vorgaben für die Benutzer unterschieden. Die technischen Vorgaben decken die Bereiche Festplattenverschlüsselung, sicheres Löschen bei Weitergabe, sicherer Zugang etc. ab, während die Benutzervorgaben Punkte wie den sicheren Transport im Auto oder die Nutzung im Homeoffice regeln.</p> <p>Speichergeräte: Neben den Regelungen, die auch für Laptops gelten, können hier Aufzeichnungen hinzukommen, wenn z.B. USB-Sticks an Lieferanten weitergegeben oder zwischen Abteilungen ausgetauscht werden. In diesen Fällen ist festzuhalten, wer welche Daten aufgrund welcher Anweisung sicher weitergegeben hat. Eine entsprechende Richtlinie regelt dabei die Vorgehensweise. Es ist sehr zu empfehlen, Daten auf mobilen Speichergeräten grundsätzlich zu verschlüsseln.</p>
Verwaltung von Benutzern Zugang zu IT-Systemen und Anwendungen (inklusive Remote-Zugang) Vergabe von Benutzerrechten	<p>Die Vorgehensweise der Auditoren folgt in diesen drei Punkten weitgehend den Vorgaben der ISO 27002 und ist umfassend in den Bemerkungen im Fragenkatalog abgebildet. Die Beantwortung dieser Vorgaben kann aufgebaut werden, indem man den Hauptphasen des Identity Management Life Cycles folgt:</p> <ol style="list-style-type: none">1. Anlage von Benutzern und initiale Rechtevergabe2. Benutzer wechseln die Abteilung oder den Verantwortungsbereich, die Benutzerrechte werden angepasst3. Benutzer scheiden aus dem Unternehmen aus und die Zugriffsrechte werden entzogen <p>Weitere Schwerpunkte sind die sichere Authentifizierung und die Autorisierung von Benutzern. Dies bezieht sich auch auf Support-Stellen, die Passwörter zurücksetzen können.</p> <p>Alle diese Punkte beziehen sich auch auf den Zugang zum Unternehmensnetzwerk per VPN-Zugang.</p>



Stichworte zum Thema	Hilfestellung
Verschlüsselung von Daten	Die eingesetzten und in den Richtlinien festgeschriebenen Verschlüsselungsstandards, die Art der Verwaltung und Distribution von Schlüsseln, die Festlegung von Schlüssellängen und die Einsatzgebiete von Verschlüsselungstechnologien sollten dokumentiert und in Richtlinien festgelegt werden. Dabei ist es sinnvoll, sich auf Stellen wie das BSI zu berufen und deren Regelungen mit einzubeziehen.
Sichere Datenübertragung	Insbesondere die Übertragung von Daten an Dritte, aber auch der interne Netzwerkverkehr, zumindest bei entsprechend hoher Einklassifizierung betroffener Daten, muss durch Maßnahmen wie die Verschlüsselung der Daten sichergestellt werden.
Change-Management	Richtlinien und Sicherheitsprozesse passen immer jeweils zu einem bestimmten Zeitpunkt auf die aktuelle Organisation und die aktuellen Prozesse innerhalb dieser Organisation. Folgerichtig kann es vorkommen, dass Richtlinien und Sicherheitsprozesse nach der Änderung der Organisation angepasst werden müssen. Was für diese übergeordneten Änderungen gilt, kann auch im Kleinen gelten. So hat der Wechsel der Software, die für das Identity Management genutzt wird, Folgen, die in Richtlinien und Prozessen abgebildet werden müssen. Damit dies funktioniert, muss es wiederum Prozesse und Ressourcen geben, die das entsprechende Change-Management durchführen.
Trennung von Entwicklungs-, Test- und Produktivumgebung	Anhand einer Übersicht aller Entwicklungsumgebungen soll jeweils die Risikoeinstufung aufgezeigt werden und der Nachweis erbracht werden, dass zumindest die höher klassifizierten Umgebungen dem Prinzip der Trennung von Entwicklungs-, Test- und Produktivumgebung folgen. Dies beinhaltet auch jeweils eigene Zugriffskonzepte und definierte Prozesse, die den Transport zwischen den Umgebungen festlegen.



Stichworte zum Thema	Hilfestellung
Logfile Management	Aufzeichnungen über administrative Tätigkeiten und die Verarbeitung von kritischen Daten sollen erstellt werden, um zum einen im laufenden Betrieb identifizierte Abweichungen in ein Security Incident Management übergeben zu können, und zum anderen, um im Nachhinein forensisch tätig werden zu können. Deshalb sind folgende Punkte nachzuweisen: <ul style="list-style-type: none">■ Welche Log-Daten werden auf welche Weise erfasst, gespeichert und zur Auswertung bereitgehalten und wer hat welche Art Zugriff auf diese Daten?■ Wie gestaltet sich der auf Log-Daten aufbauende Security-Incident-Management-Prozess?■ Wie werden die Daten ausgewertet, falls z.B. ein Angriff auf das Benutzerverzeichnis im Nachhinein aufgearbeitet werden muss?
Schutz vor Schadsoftware	Die regelmäßig im Zusammenhang mit dem Punkt »Schadsoftware« abgefragten Dokumente umfassen: <ul style="list-style-type: none">■ die entsprechenden Richtlinien und Handlungsanweisungen,■ Schulungsunterlagen für Benutzer■ und den Nachweis des Installationsstatus entsprechender Antiviren-Software auf den eingesetzten Gerätschaften.
Schwachstellenmanagement	Im Rahmen des Assetmanagements werden die verschiedenen eingesetzten Betriebssysteme und Softwareprodukte gelistet. Jedem dieser Assets stehen mögliche Bedrohungen gegenüber. Erst zusammen mit einer oder mehreren Schwachstellen wird eine Bedrohung zu einem Risiko. Im Zusammenhang mit dieser Frage ist darzustellen, wie Schwachstellen von Software oder auch Zutrittssystemen gesucht und behandelt werden.



Stichworte zum Thema	Hilfestellung
	<p>Eine der wichtigsten und häufigsten Schwachstellen ist das Fehlen aktueller Softwareversionen oder Patches, weshalb immer die beiden folgenden Fragen zu beantworten sind:</p> <ul style="list-style-type: none">■ Auf welche Art und Weise werden fehlende Patches oder nicht mehr unterstützte Software identifiziert? (Das kann z.B. durch einen Schwachstellenscanner automatisiert geschehen oder aber durch regelmäßige Inventur.)■ Welche Prozesse und Richtlinien sind implementiert, um bekannt gewordene Schwachstellen zu beseitigen?
Überwachung und Überprüfung von IT-Systemen (IT-Systemaudit)	<p>Diese Frage geht über den Punkt »Schwachstellenmanagement« hinaus und bezieht zusätzlich folgende Bereiche mit ein:</p> <ul style="list-style-type: none">■ Audits von Plattformen und IT-Systemen mit dem Ziel, die Einhaltung der Richtlinien zu überprüfen■ Fokus auf Bereiche wie das Benutzermanagement, die Trennung von Mandanten, Verschlüsselung von Daten oder die Härtung von Betriebssystemen <p>Die geforderte Ausdetaillierung der Fragen und damit auch der Antworten ist abhängig von der Kritikalität des Systems.</p>
Netzwerkmanagement	<p>Die bildliche Darstellung des lokalen Netzwerkes im Rahmen einer Übersicht und die detailliertere Darstellung der Trennung von Netzwerken wie z.B. die Trennung von Büronetzwerk und Produktionsnetzwerk sind eine wichtige Grundlage für den Auditor, um den Umfang und die Komplexität des Unternehmensnetzwerks und damit der Datenkommunikation zu verstehen. Auf diesem Dokument und den entsprechenden Richtlinien aufbauend wird abgefragt, wie die Verwaltung der aktiven und passiven Netzwerkkomponenten stattfindet, wie neue Geräte Zugang erhalten und wie die Anbindung von externen Partnern, inklusive Cloud-Dienstleistern, eingerichtet und überwacht werden.</p>



Stichworte zum Thema	Hilfestellung
Netzwerkdienste	Neben dem reinen Datenverkehr werden im Netzwerk auch häufig Telefone oder Echtzeitanwendungen betrieben. Um die jeweiligen Anforderungen an jeden dieser Services zu gewährleisten, ist es üblich, entsprechende Service Level Agreements (SLA) abzuschließen, die den Benutzern des Netzwerks eine garantierte Qualität zusichern. Dieser Punkt ist Teil des Feldes »Verfügbarkeit« und soll ermitteln, inwieweit der Zugriff auf Kundendaten gewährleistet wird.
Löschen von Daten bei externen Dienstleistern (z.B. bei Cloud-Betreibern)	Informationen durch externe Stellen verarbeiten zu lassen, ist weitverbreitet und deshalb muss bereits beim Abschluss eines entsprechenden Vertrags geregelt werden, wie mit den Daten zu verfahren ist, wenn die Vertragsbeziehung – aus welchen Gründen auch immer – beendet wird. Das betrifft zum einen das Löschen der Daten, zum anderen aber auch das »Zurückholen« im Falle des Wechsels des Anbieters oder bei dessen Konkurs. Dieser Punkt ist eng mit dem Recht auf Vergessen aus der EU-DSGVO verbunden. Ist es schon schwierig, die individuellen, personenbezogenen Daten einer Person aus einer Datenbank zu entfernen, die im eigenen Rechenzentrum betrieben wird, so steigt der Aufwand bei einer Cloud-Lösung stark an.
Separierung von Daten bei externen Dienstleistern (z.B. bei Cloud-Betreibern)	Ein Public-Cloud-Betreiber hat in der Regel viele Kunden, die häufig in einer Konkurrenzsituation zueinander stehen. Aus diesem Grund ist es wichtig, dass externe Dienstleister darstellen können, inwieweit die Daten der verschiedenen Kunden physisch oder per Berechtigungs- und Mandantenkonzept voneinander getrennt gespeichert und verarbeitet werden.
Sichere Softwareentwicklung	Die Entwicklung von Software wird in der Regel in Form eines Projekts strukturiert. Das Thema Security muss in den entsprechenden Projektphasen Beachtung finden und dabei den Vorgaben einer Richtlinie folgen. Als Grundlage einer solchen Richtlinie empfiehlt es sich, den gängigen Standards zu folgen.



Stichworte zum Thema	Hilfestellung
Anbahnung von Geschäftsbeziehungen	<p>Bevor Daten mit einem externen Dienstleister ausgetauscht werden, erfolgen üblicherweise Einkaufsprozesse wie die Lieferantenauswahl und -bewertung. Die dabei üblichen Kriterien, wie z.B. die Lieferqualität, müssen um Kriterien der IT-Security ergänzt werden. Dazu könnte auch gehören, dass der Fragenkatalog ausgefüllt und die Angaben durch die Unternehmensleitung bestätigt werden müssen.</p> <p>Ein Ziel von TISAX ist die Überprüfung der gesamten Lieferkette. Deshalb werden immer mehr Lieferanten dazu übergehen, wiederum ihre Unterlieferanten einem TISAX-Audit zu unterziehen. In den Lieferbedingungen den Vorweis eines TISAX-Testats festzuschreiben, ist deshalb eine valide, wenn auch aktuell noch weitgehend unrealistische Möglichkeit der Prüfung.</p>
Compliance	<p>Dieser Punkt fragt ab, wie das Unternehmen sicherstellt, dass alle infrage kommenden gesetzlichen und normativen Anforderungen an das Unternehmen bekannt sind und befolgt werden.</p> <p>Diesem Punkt begegnet man z.B., indem man zunächst nachweist, dass die relevanten Gesetze bekannt sind. So kann ein Register geführt werden, das diese Gesetze beinhaltet und im besten Fall bereits auf Maßnahmen verweist. Auch ein sogenannter »Law-Tracking-Service« dient dem Nachweis, dass man sich als Unternehmen laufend über Änderungen der Gesetzeslage informiert.</p>





4 Organisation von Richtlinien

4.1 Kapitelzusammenfassung

Richtlinien formulieren Vorgaben an die verschiedenen Mitarbeitergruppen und beschreiben damit, wie sie sich in Bezug auf die Sicherstellung von Informationssicherheit verhalten müssen. Verschiedene Rollen der angesprochenen Mitarbeiter erfordern jeweils angepasste Richtlinien. Ein IT-Mitarbeiter wird demnach ausführlichere technische Vorgaben z.B. bezüglich der Konfiguration von IT-Systemen benötigen, wohingegen ein Mitarbeiter der Ver sandabteilung wissen möchte, was er zu Hause mit seinem Unternehmens-Laptop machen darf.

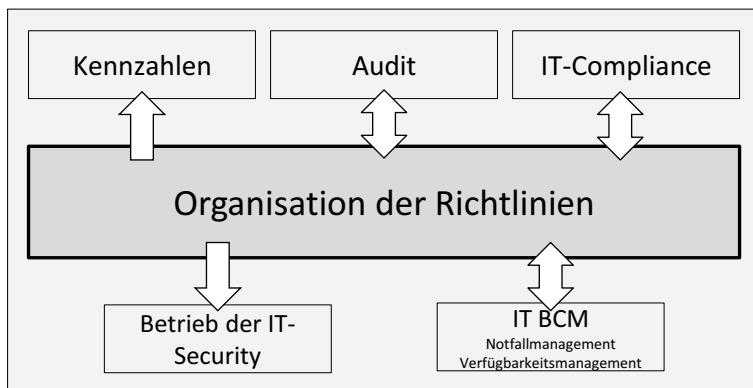


Abbildung 4.1: Primäre Abhängigkeiten von anderen Themen der IT-Security

Die Top-6-Fragen zum aktuellen Kapitel:

- Wurden die von den verschiedenen Normen geforderten Basisrichtlinien erstellt, durch das Management abgenommen und dem betroffenen Personenkreis kommuniziert?
- Wurden die weiteren grundlegenden Richtlinien wie die Klassifizierungsrichtlinie, die Notfallrichtlinien oder die Richtlinie zum IT-Risikomanagement erstellt, von der Unternehmensleitung abgesegnet und verteilt?



KAPITEL 4 – ORGANISATION VON RICHTLINIEN

- Wurden Richtlinien für den sicheren IT-Betrieb erstellt und getestet?
- Wurden Richtlinien für Benutzer, die den Umgang mit Gerätschaften, E-Mail und dem Internet regeln, erstellt und kommuniziert?
- Ist technisch sichergestellt, dass Mitarbeiter zu jeder Zeit auf die aktuelle Version einer Richtlinie Zugriff haben?
- Ist sichergestellt, dass die in den Richtlinien festgelegten Vorgaben von den betroffenen Mitarbeitern auch technisch und organisatorisch umgesetzt werden können?

4.2 Einführung

4

Ohne die fortlaufende Überprüfung von Prozessen, IT-Systemen oder allgemein ausgedrückt des Sicherheitslevels kann es keine zielgerichteten Verbesserungen geben. Maßnahmen werden aufgrund von Abweichungen von Sicherheitszielen definiert und implementiert. Nur was bedeutet »Abweichungen«? Abweichungen stellen das Delta zwischen dem definierten Soll-Zustand und einem Ist-Zustand dar. An dieser Stelle gewinnen Richtlinien an Bedeutung. Sie definieren den zu erreichenden Soll-Zustand und sind damit die Messlatte für den Zustand von sicherheitsrelevanten Systemen. Audits prüfen anhand von Richtlinien, ob Abweichungen vorliegen. Mitarbeiter richten anhand von Richtlinien ihr Verhalten mit sensiblen Daten aus, und nicht zuletzt werden bei Fehlverhalten hinsichtlich der IT-Security-Vorgaben, festgelegt in Richtlinien, personalrechtliche Konsequenzen folgen. Damit bilden Richtlinien das formale Fundament des IT-Security-Managements.

Das Wort »Richtlinie« wird als Synonym zur Bezeichnung »Policy« benutzt. Ein Unterschied zwischen den beiden Ausdrücken wird nicht gemacht. Aus dem englischen Sprachraum kommend hat sich der Begriff »Policy« von Mitte der 90er Jahre an schnell verbreitet.

Häufig ist auch die Bezeichnung »Leitlinie« zu finden. Auch wenn dieses Wort häufig synonym zu »Policy« oder »Richtlinie« genutzt wird, sind dabei aber doch Unterschiede zu beachten. Eine Leitlinie ist im Grunde eine Feststellung oder Beschreibung, die eine Entscheidung unterstützen soll. Eine Richtlinie dagegen hat verbindlichen Charakter bzw. legt Prozesse und technische Vorgehensweisen formal fest. Das Dokument, das in der DIN 27001 auch als »ISMS-Leitlinie« bezeichnet wird, ist die Sicherheitsrichtlinie. Die-



ses oberste Dokument enthält keine Ratschläge, sondern legt die Bedeutung der IT-Security für das Unternehmen aus Sicht der Unternehmensleitung wegweisend fest. Ob nun der Begriff »Leitlinie« angebracht ist oder nicht, bleibt dahingestellt, im vorliegenden Buch bleibt es durchgängig beim Begriff »Richtlinie«, um Missverständnissen vorzubeugen.

4.3 Strukturierung von Richtlinien

Richtlinien bauen aufeinander auf und sollten deshalb hierarchisch strukturiert werden. In diesem Zusammenhang spricht man von einer »Richtlinien-Pyramide«. Gleichzeitig ist der Blick auf und die Erwartung an die Sicherheitsrichtlinien durchaus unterschiedlich. Ein Geschäftsführer, der gewährleisten muss, dass alle erforderlichen Vorkehrungen zur Sicherstellung der Datensicherheit getroffen wurden, konzentriert sich auf Richtlinien einer anderen Stufe als der Mitarbeiter aus dem Support, der wissen muss, wie die Sicherheitseinstellungen an einem Laptop zu konfigurieren sind. Das betrifft zum einen den reinen Inhalt, zum anderen aber auch den Aufbau, die Sprache und die Detailtiefe.

In Unternehmen mit vielen Standorten kommt oftmals hinzu, dass standortspezifische Richtlinien existieren, die in die Gesamthierarchie eingebunden werden müssen. In diesen Fällen empfiehlt es sich, diese weitgehend zu standardisieren. So können Regelungen wie z.B. der Umgang mit E-Mail-Postfächern in der einen Lokation alleine schon aufgrund von Datenschutzgesetzen existieren, die an anderen Standorten bzw. in anderen Ländern nicht vorhanden sind. In diesem Fall könnte man sich eine einzige Richtlinie vorstellen, die sich mit dem allgemeinen Umgang mit E-Mail beschäftigt und alle standortspezifischen Abweichungen in eigenen Kapiteln aufzählt. Natürlich kann auch aus dem Dokument auf entsprechende weiterführende Dokumente verwiesen werden. Im Grunde ist nur entscheidend, dass derjenige, der Informationen benötigt, diese auch finden kann.

In Abbildung 4.2 ist eine beispielhafte Richtlinien-Pyramide abgebildet. Die oberste Ebene enthält alle Richtlinien, die üblicherweise von der Unternehmensleitung angefordert, genehmigt und auch unterschrieben werden. Damit beschreiben und repräsentieren sie den Auftrag zum Aufbau und Betrieb des IT-Security-Managements. Auf diesen Top-Level-Dokumenten bauen alle untergeordneten Dokumente auf – deshalb auch die Form einer Pyramide.



KAPITEL 4 – ORGANISATION VON RICHTLINIEN

Damit wird auch schnell deutlich, dass es schwer ist, Richtlinien, also verbindliche Vorgaben, zu entwickeln, wenn der Auftrag in Form der Sicherheitsrichtlinie fehlt.

4

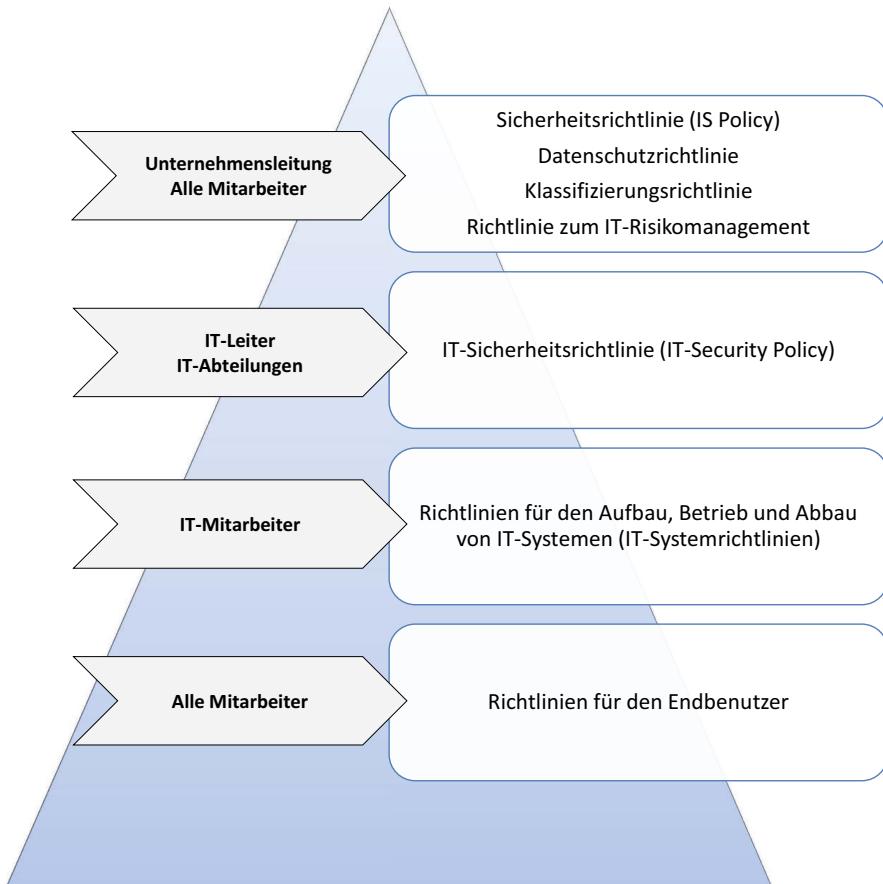


Abbildung 4.2: Richtlinien-Pyramide

4.4 Beschreibung und Kategorisierung

Für eine spätere erfolgreiche Recherche innerhalb eines größeren Fundus an Dokumenten ist es erforderlich, Ordnungskriterien festzulegen. Dabei kann man sich an wissenschaftlichen Klassifikationssystemen orientieren. Eine Reihe von Attributen wird deshalb jedem Dokument mitgegeben. Dazu gehören zumindest der Verfasser, das Datum, die Stelle, die das Dokument



freigegeben hat, ein Titel, eine Beschreibung, die Versionsnummer und der Geltungsbereich. Diese Attribute beschreiben Zweck und Reichweite eines Dokuments und helfen maßgeblich dabei, dass jeder Befugte in der Lage ist, die von ihm benötigten Richtlinien innerhalb einer angemessenen Zeitspanne zu finden.

Ein weiterer Faktor ist die Erforderlichkeit, dass dafür Sorge getragen wird, dass jeweils auf die aktuelle Version eines Dokuments zugegriffen wird. Bei Dokumenten, die sehr techniknahe Details beschreiben, kann dies durchaus eine schwierige Aufgabe darstellen, da häufige Änderungen, unter Umständen durch eine Vielzahl unterschiedlicher Personen, eine Vielzahl von Versionen hervorbringen. Werden diese verschiedenen Versionen nicht an einer zentralen Stelle abgelegt, so sind Fehler vorprogrammiert.

Neben den oben erwähnten Attributen benötigen vor allem technische Beschreibungen ein weiteres Attribut, das die Verbindung zu einem IT-System oder einer Software möglich macht. Die Konfigurationsbeschreibung für eine bestimmte Software ist wenig hilfreich, wenn nach einiger Zeit in Vergessenheit gerät, um welche Software in welcher Version es sich dabei gehandelt hat. Außerdem wird es dadurch schwierig, alle zu dieser Software gehörenden Dokumente aufzuzeigen.

Die Beschreibung und Kategorisierung von Dokumenten anhand von Attributen wird stark erleichtert, wenn nicht nur das Deckblatt einer Richtlinie mit den eben genannten Attributen geschmückt wird, sondern sie als durchsuchbare Metadaten angelegt werden. Dazu sind entsprechende Funktionalitäten erforderlich, wie sie bei einem Dokumentenmanagementsystem zu finden sind.

4.5 Pflege und Lenkung von Richtlinien

Grundsätzliche Aufgabe der Dokumentenlenkung ist die Bereitstellung der jeweils aktuellen Version eines Dokuments für jede berechtigte Stelle. Das bedeutet aber auch, dass der unbefugte Zugriff, die unbefugte Änderung und das unbefugte Löschen durch technische Maßnahmen verhindert werden müssen.

Um diese Anforderungen abdecken zu können, sollten verschiedene Prozesse etabliert werden. Diese Prozesse werden unter dem Oberbegriff »Ände-



KAPITEL 4 – ORGANISATION VON RICHTLINIEN

rungsmanagement« (engl. Change Management) zusammengefasst. Das betrifft nicht nur Richtlinien, sondern genauso Protokolle von Besprechungen, von Änderungen an IT-Systemen oder Software oder Bedienungsanleitungen. Nur wenn jede beteiligte Person weiß,

- wann sie ein Dokument anzulegen hat,
- wer darauf Zugriff erhalten soll,
- wie dieses aussehen muss und
- wie es abzulegen ist,

kann es ein stringentes und vollständiges System zur Lenkung von Dokumenten geben.

4

Tipp

Für alle vier Punkte sollte es Vorlagen und entsprechende Anweisungen geben. Es ist zudem von Vorteil, wenn anstelle von Papierunterlagen bereits vorgefertigte elektronische Formulare zum Einsatz kommen. Dadurch können Fehleingaben und allgemein Missverständnisse stark reduziert werden.

Die Freigabe von Dokumenten muss in den meisten Fällen einem geregelten Genehmigungsprozess unterworfen werden. Änderungen an Dokumenten wie der Sicherheitsrichtlinie sollten dabei von Mitgliedern der Unternehmensleitung oder einem von ihr dazu autorisierten Gremium abgesegnet werden, Änderungen an Notfallplänen häufig sowohl von der IT-Leitung als auch vom Controlling. Auf diese Weise kann jeder Dokumentenkategorie ein Prozess zur Abnahme der Dokumente zugewiesen werden. Der Abnahmeprozess kann dabei durch den Einsatz von elektronischen Workflows unterstützt werden.

Manchmal heißt es auch hier: »Weniger ist mehr«. Ein überbordendes System an Workflows und Prozessen rund um die Erstellung und Pflege von Dokumenten kann zu Aufwänden führen, die nicht mehr sinnvoll aufgebracht werden können, und nicht selten führt dies zum kompletten Stillstand. Aus diesem Grund sollte mit Augenmaß entschieden werden, welche Klassen von Dokumenten auf welchem Weg in das ISMS integriert werden sollen.



Ein weiterer Grund für den Aufwand, den ein solches System generiert, ist die erforderliche Vorgabe, dass Dokumente aktuell zu halten sind. Ein System zur Versionierung, wie es in der Softwareentwicklung üblich ist, kann dabei helfen. Werden Änderungen vorgenommen, so kann auch in diesem Fall wieder eine Abnahme erforderlich werden. Auch in diesem Punkt sollte definiert sein, wann dies geschehen muss.

Dokumente, die sehr selten modifiziert werden (die Basisrichtlinien sind solche Dokumente), sollten einem regelmäßigen Änderungsmechanismus unterworfen sein. In diesem speziellen Fall könnte alle zwei Jahre eine Überprüfung und Abnahme stattfinden.

Sind Dokumente abgelegt, mit Attributen beschrieben und innerhalb des ISMS mit Unternehmenswerten oder Prozessen verknüpft, dann sollten alle Berechtigten in der Lage sein, jeweils das passende Dokument in der aktuellen Version aufzurufen. Wird ein Dokument gefunden und ist die erforderliche Software zur Anzeige auf dem Bildschirm vorhanden, dann entscheiden auch Form, Inhalt und Struktur darüber, ob das Dokument bei der Lösung der aktuellen Fragestellung helfen kann. Standards und vorgefertigte Templates helfen dabei, diese Voraussetzungen zu schaffen.

Sehr häufig sind Dokumente in Unternehmen anzutreffen, die ganz offensichtlich vor einiger Zeit erstellt wurden, oft von Externen, danach aber nicht mehr angepasst wurden. Das kommt z.B. dann zustande, wenn im Rahmen eines Projekts eine Richtlinienstruktur aufgebaut wird, der Übergang zum Betrieb aber nicht in korrekter Form stattfindet. Grundsätzlich gilt, dass die Pflege von Dokumenten über einen längeren Zeitraum schnell zeitintensiver und kostenintensiver ist als die Ersterstellung. Dazu kommt, dass nur ein kontrollierter Pflegeprozess dafür Sorge tragen kann, dass vorhandene Richtlinien ihren Zweck erfüllen. Im Grundsatz kann man sagen, dass einige wenige wirklich gelenkte Dokumente häufig sinnvoller sind als Hunderte, die eine reine Alibifunktion wahrnehmen.

4.6 Richtlinien und Audits

Richtlinien und Audits stehen in einem Abhängigkeitsverhältnis zueinander. Nachvollziehbarerweise kann es keine Überprüfung von Sachverhalten geben, ohne einen Maßstab bereitzustellen, anhand dessen eine Messung durchgeführt werden kann.



KAPITEL 4 – ORGANISATION VON RICHTLINIEN

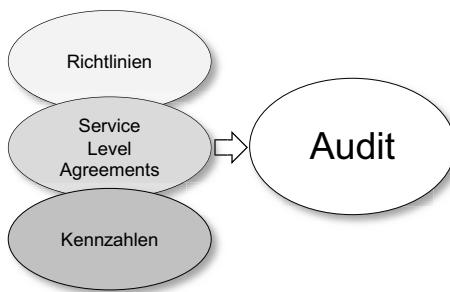


Abbildung 4.3: Voraussetzungen für die Durchführung eines Audits

4

Richtlinien legen die Grundregeln fest, die mithilfe von Kennzahlen in quantifizierbare und messbare Zahlen übersetzt werden können. Ein Audit baut darauf auf. Natürlich ist es auch möglich, Überprüfungen ohne Kennzahlen durchzuführen. Aber wenn es letztendlich darum geht, Vergleichbarkeit zwischen den Ergebnissen verschiedener Messungen zu unterschiedlichen Zeitpunkten oder Ergebnissen verschiedener Standorte herzustellen, wird ein möglichst objektives Maßsystem erforderlich werden. Deshalb ist es zudem sinnvoll, bereits bei der Verfassung von Richtlinien, zumindest wenn es sich um technische Sachverhalte dreht, bereits mit konkreten Zahlen zu arbeiten. Eine Vorschrift zur Installation von Antivirenprogrammen kann damit mit dem Maß »Abdeckungsgrad in % bei Arbeitsplatzmaschinen« arbeiten oder die Festlegung eines sich automatisiert einschaltenden Bildschirmschoners mit Passwortschutz mit einer Anzahl an Minuten.

Als Grundlage von Audits kommen neben den internen Richtlinien verstärkt Vorgaben von außen hinzu. Dazu gehören die Vorschriften vonseiten des Gesetzgebers, des Kunden oder des Branchenverbandes. Insbesondere die Anstrengungen, innerhalb einer Branche ein vergleichbares Sicherheitsniveau herzustellen, werden nicht nur durch die beteiligten Firmen, sondern durchaus auch von den Regierungen intensiviert. Aktuell betrifft es vor allem diejenigen Branchen, die kritische Infrastrukturen, wie Kraftwerke oder den Verkehr, bereitstellen. Weitere typische Beispiele sind Unternehmen, die in großem Umfang personenbezogene Daten speichern und verarbeiten, oder Bereiche, die als Know-how-Träger gelten. So organisiert der Verband der Automobilindustrie (VDA) ein eigenes Audit- und Zertifizierungssystem, das Trusted Information Security Assessment Exchange (TISAX). Innerhalb des VDA werden dazu, eng an den ISO-27001-Standard angelehnt, eigene Fragenkataloge entwickelt und beteiligte Unternehmen angeregt, sich einem



darauf basierenden Zertifizierungssystem zu unterwerfen. Das Ziel ist hierbei, ein gleichbleibend hohes, an international anerkannten Standards ausgerichtetes Sicherheitsniveau zu erreichen. Im Zuge der steigenden Risiken durch anfällige Software in Automobilen ist dies der richtige Schritt und dürfte deshalb nur ein Vorläufer für weitere Schlüsselbranchen darstellen. In Kapitel 3 »IT-Compliance« gehe ich näher darauf ein.

4.7 Verschiedene Richtlinien

Die Top-Level-Richtlinien, die in Abbildung 4.2 aufgeführt sind, bilden das Fundament für alle weiteren Richtlinien. Natürlich wird jedes dieser Dokumente stark von Unternehmen zu Unternehmen variieren, aber dennoch haben sich die Anforderungen an die grundlegenden Inhalte in den letzten Jahren weiter verfestigt. Beispielhaft werden in den nächsten Abschnitten einige grundlegende Richtlinien detaillierter beschrieben und auch exemplarisch skizziert. Ausgegangen wird dabei von einem mittelständischen bis großen Unternehmen mit Zweigstellen im Inland oder auch Ausland.

In kleinen Unternehmen finden sich oft Dokumente, die alle Inhalte auf einmal zusammenfassen. In sehr großen Unternehmen wiederum geht die Tendenz eher in die Richtung, zu diversifizieren. Das liegt meistens daran, dass, je größer das Unternehmen ist, auch die Anzahl derjenigen anwächst, die an der Erstellung und vor allem Pflege der Dokumente beteiligt sind, was wiederum fast zwangsläufig seinen Niederschlag in der Komplexität der Richtlinienstruktur findet. Diese Beispiele sollen deutlich machen, dass es die perfekten Richtlinien nicht gibt und dass die Größe eines Unternehmens wie auch andere Rahmenbedingungen (z.B. der Geschäftszweck) einen großen Einfluss auf die Ausgestaltung dieser Dokumente hat.

Richtlinien entstehen nicht aus dem Nichts. Zum einen entwickeln sie sich parallel zum sich schnell verändernden IT-Security-Management, und zum anderen richten sie sich nach Standards und Gesetzen. Die IT-Compliance-Vorgaben aus den verschiedensten Richtungen spielen also eine große Rolle. Fordert der Gesetzgeber oder noch häufiger der Kunde eine bestimmte Maßnahme, so findet sich diese oft auch in einer Richtlinie wieder. Das beginnt bei der grundsätzlichen Forderung nach einer IT-Security-Organisation und reicht bis hin zum Umgang mit Kundendaten auf allen technischen Ebenen.



KAPITEL 4 – ORGANISATION VON RICHTLINIEN

Alle maßgeblichen Standards, die auch den Aufbau und Betrieb eines Information-Security-Management-Systems (ISMS) beschreiben, fordern auch den Aufbau und die Weiterentwicklung von Richtlinien. Die nachfolgenden Richtlinien sind demzufolge sowohl an die ISO-2700x-Normen wie auch an die Vorgaben des BSI angepasst. Ist das Unternehmen z.B. auch den Regelungen des Sarbanes-Oxley Acts (SOX) unterworfen, so kann eine dementsprechende Richtlinie zur Dokumentation von Änderungen an Rechten und zur Überwachung von administrativen Tätigkeiten direkt in die Richtlinien-Pyramide mit aufgenommen werden.

4.7.1 Sicherheitsrichtlinie

4

Die Sicherheitsrichtlinie wird auch unter den Bezeichnungen »Leitlinie zur Informationssicherheit« in der ISO-27001-Norm, als »Information Security Policy« in der englischen Literatur oder als »Sicherheitsleitlinie« gefunden. Im Deutschen nennt sich diese Richtlinie »Informationssicherheitspolitik«. Dieser Begriff »Politik« wurde im Zusammenhang mit dieser Richtlinie ganz bewusst gewählt, um sie von den anderen Richtlinien abzugrenzen. Es dreht sich in diesem Dokument dann auch alles eher um die politische Dimension innerhalb eines Unternehmens, wenn es um die Haltung der Unternehmensleitung hinsichtlich der Informationssicherheit geht oder wenn Kompetenzen wie die Richtlinienhoheit an definierte Stellen verteilt werden. Um der Verwirrung keinen Vorschub zu leisten, bleiben wir beim Begriff »Sicherheitsrichtlinie«. Das Wort Richtlinie hat dabei einen verbindlichen Charakter, und das ist angemessen für dieses Dokument. Natürlich ist sie trotzdem, vor allem hinsichtlich der richtungsweisenden Funktion, auch eine Leitlinie.

Die Sicherheitsrichtlinie ist die oberste Richtlinie eines Unternehmens und damit das Fundament für das IT-Security-Management.

Wichtig

Die gemäß der ISO 27001 verbindlich zu erstellende »IS-Politik« – die Sicherheitsrichtlinie – ist ein Dokument, das im Zertifizierungsprozess eine wichtige Rolle spielt. Unternehmen, die keine Zertifizierung nach ISO 27001 anstreben, können die Inhalte auch weniger formal dokumentieren. Nichtsdestotrotz ist die Selbstverpflichtung der Unternehmensleitung, Informationssicherheitsziele anzustreben, essenziell und sollte in diesem oder einem ähnlich aufgebauten Dokument schriftlich fixiert werden.



Es kann nicht häufig genug erwähnt werden, wie wichtig die Sicherheitsrichtlinie bzw. die darin dokumentierten Prinzipien für das IT-Security-Management und die Erreichung eines angestrebten Sicherheitsniveaus ist. Die Bedeutung spiegelt sich im Inhalt wider. Grundsätzlich sollten zumindest die folgenden Bereiche abgedeckt werden:

- Die Unternehmensleitung betont die Wichtigkeit der Informationssicherheit für das Unternehmen. An dieser Stelle kann eine Verbindung zu den Unternehmenszielen hergestellt werden.
- Der Geltungsbereich der Sicherheitsrichtlinie wird definiert. Im Idealfall wird selbst in sehr großen Unternehmen nur eine solche Richtlinie definiert.
- Die Unternehmensleitung ist Treiber und Prüfer der Maßnahmen hinsichtlich des Schutzes von Daten des Unternehmens, der Kunden und Lieferanten.
- Die allgemeinen Ziele der IT-Security werden skizziert. Falls das IT-Security-Management Standards befolgt, so können diese genannt werden. Ist eine Sicherheitsstrategie definiert, dann sollte diese auch kurz Erwähnung finden.
- Die Kompetenzen der IT-Security-Organisation werden aufgezeigt. Ein typisches Beispiel ist die Zuweisung der Richtlinienhoheit und eine Beschreibung des Freigabeprozesses. Im gleichen Schritt wird die Verantwortung jedes einzelnen Mitarbeiters hinsichtlich des Schutzes von Unternehmenswerten betont. Der Aufbau und die organisatorische Eingliederung der IT-Security-Organisation werden aufgezeigt.
- Ein Verweis auf andere Top-Level-Dokumente wie die Klassifizierungsrichtlinie, das ISMS-Handbuch oder die Richtlinie zum IT-Risikomanagement.
- Abschließend werden Formalien wie die Intervalle zur Wartung der Richtlinie beschrieben.

Die aufgezählten Bereiche sollten knapp gehalten werden, viele derartige Dokumente sind nur wenige Seiten lang. Falls es sich als problematisch erweist, Sachverhalte in nur wenigen Sätzen auszuführen, oder wenn ausdrücklich eine ausführliche Ausarbeitung gewünscht ist, ist es sinnvoll, diese Bereiche in ein eigenes Dokument, wie das ISMS-Handbuch zu überführen.



Sicherheitsrichtlinie der Firma ABC	
Verantwortung der Unternehmensleitung	Wir sehen es als Grundlage unseres unternehmerischen Handelns an unsere Betriebs- und Geschäftsgeheimnisse zu schützen. Der Schutz von durch Kunden und Partner bereitgestellten Informationen ist uns hierbei genauso wichtig wie der Schutz eigenen Know-hows.
Geltungsbereich	Die vorliegende Richtlinie ist für die gesamte Unternehmensgruppe gültig.
Zielsetzung und Umfang	Ziel der Sicherheitsrichtlinie ist es, Informationen vor internen und externen Bedrohungen zu schützen, die Fortführung des Geschäftsbetriebes zu unterstützen und mögliche Schäden durch Sicherheitsvorfälle weitgehend zu minimieren. Informationen können in vielfältiger Form vorliegen. Dazu gehören elektronisch gespeicherte oder übermittelte Daten sowie Informationen auf Papier.
Sicherheitsziele	Die Sicherheitsziele sind Vertraulichkeit, Integrität und Verfügbarkeit von Unternehmensdaten und IT-Systemen.
Grundlegende Standards	Grundlage für die Auswahl von technischen und organisatorischen Maßnahmen sind die Forderungen des Regelwerkes ISO/IEC 27001 und die Standards des Bundesamtes für Sicherheit in der Informationstechnologie.
IT-Security-Organisation und ihre Kompetenzen	Die Organisationseinheit Information Security (IS) definiert Richtlinien im Bereich der Informationssicherheit und überwacht deren Umsetzung. IS ist direkt der Unternehmensleitung unterordnet und berichtet an diese.
Verantwortung der Leitungsebenen	Die Bereichs- und Abteilungsleiter sind verantwortlich für die Einführung, Einhaltung und Überwachung der Sicherheitsrichtlinie und der davon abgeleiteten Richtlinien in ihren jeweiligen Zuständigkeiten.
Verantwortung jedes einzelnen Mitarbeiters	Jeder Mitarbeiter ist selbst verantwortlich für die Einhaltung der ihn betreffenden Regelungen der Sicherheitsrichtlinie und der davon abgeleiteten Richtlinien.
	Unterschriften der Mitglieder der Unternehmensleitung

Abbildung 4.4: Exemplarische Sicherheitsrichtlinie

Bei Unternehmen, deren Unternehmenszweck darin besteht, Dienstleistungen für Kunden zu erbringen, wie es z.B. bei einem typischen Web-Hoster der Fall ist, wird der Bereich der Verantwortung des Unternehmens und der Kunden ausführlicher ausfallen als bei einem Unternehmen aus dem produzierenden Sektor. In diesem Fall kann von der Sicherheitsrichtlinie ausgehend ein Link zu einem zweiten Dokument eingetragen werden, in dem dieser Bereich ausführlich definiert wird. Im Normalfall sollte dies aber nicht Bestandteil dieses Dokuments sein, und es ist auch nicht Zweck dieser Richtlinie, Maßnahmen oder technische Sachverhalte zu behandeln.



In Abbildung 4.4 wird beispielhaft eine Sicherheitsrichtlinie dargestellt. Jeder Absatz bildet dabei, kurz und knapp gehalten, eines der Themen ab, die eine solche Richtlinie enthalten sollte. Im Folgenden gehen wir die Punkte durch:

- **Verantwortung der Unternehmensleitung:** Die Sicherheitsrichtlinie soll herausstellen, dass Informationssicherheit ein wichtiges Ziel des Unternehmens darstellt und warum dies der Fall ist. Dabei kann es sich um den Schutz von Informationen als grundsätzlicher Faktor zum Schutz des Know-hows oder aber, abhängig vom Unternehmenszweck, auch um die Wahrung von Kundendaten handeln, die im Fokus des Geschäftsbetriebs liegen. Aufgrund der Generalität dieser Aufgabenstellung ist zu betonen, dass die Sicherheitsrichtlinie für das Unternehmen und für alle Mitarbeiter spricht und dabei beide Parteien in die Verantwortung nimmt. Informationssicherheit ist kein IT-Thema, sondern ein Thema der Unternehmensführung. Das Gleiche gilt auch für ein Projekt des IT-Security-Managements, und die Sicherheitsrichtlinie ist dementsprechend die Grundlage für ein solches Projekt.
- **Geltungsbereich (scope):** Der Geltungsbereich der Sicherheitsrichtlinie ist der nächste wichtige Punkt. Gelten die Vorgaben für das gesamte Unternehmen? Sind Tochterunternehmen automatisch Bestandteil des Geltungsbereichs? Für den Fall, dass Unternehmensteile oder einzelne Bereiche von diesen Vorgaben ausgenommen werden, sollte dies hinreichend klar beschrieben werden. Dies ist in multinational agierenden Unternehmen durchaus eine Herausforderung, weil es gleichzeitig bedeutet, dass die Sicherheitsrichtlinie zwischen den Unternehmensteilen abgestimmt werden muss, bevor sie verabschiedet wird. Es kann vorkommen, dass Tochterunternehmen weit gravierenderen Sicherheitsbestimmungen unterworfen sind als ein Großteil des übrigen Unternehmens. In Fällen, in denen nur Teile des Unternehmens sensible Kunden betreuen oder z.B. Rüstungsaufträge bearbeiten, können Bestimmungen bestehen, die tiefgreifender sind als diejenigen, die der allgemeinen Sicherheitsrichtlinie zugrunde liegen. Um der Aufgabe als Top-Level-Dokument gerecht zu werden, ist es sinnvoll, diese Zusammenhänge deutlich aufzuzeigen.
- **Zielsetzung und Umfang:** Nun folgt eine Erklärung, warum das Dokument wichtig ist und warum es hilft, Informationssicherheit zu etablieren. Das Dokument existiert nicht als Selbstzweck, sondern um realen Bedrohungen zu begegnen, die Informationen und damit das Know-how des Unternehmens gefährden. Das hat ganz entscheidend etwas mit der Stellung im



Wettbewerb und der Demonstration von Vorsorge zu tun. Es reicht also nicht, eine organisatorische Stelle zu schaffen und ihr den Titel »IT-Security« zu geben. In diesem Dokument wird betont, wie diese Stelle und die damit verbundenen Aufgaben nachhaltig unterstützt werden sollen.

- **Sicherheitsziele:** Der nächste Teil der Richtlinie kann sich damit beschäftigen, was denn zu schützen ist. Der Wert »Information« kann weit gefasst oder aber auch auf IT-Daten reduziert werden. Ist ein Unternehmen im Bereich des Maschinenbaus tätig, dann kann auch ein neuer Prototyp eines Werkzeugs ein Träger von schützenswerten Informationen sein. Genauso wie die Informationen auf Papier, die diesem Prototyp beigelegt sind. Sind die schützenswerten Werte definiert, so ist zu klären, wie deren Wichtigkeit und damit der Schutzbedarf zu bestimmen ist. An dieser Stelle kann eine Klassifizierungsrichtlinie und eine Vorgehensweise zum Risikomanagement erwähnt werden. Oftmals werden Schutzziele wie Vertraulichkeit, Verfügbarkeit und Integrität genannt und erläutert, um an dieser Stelle zu dokumentieren, welche Kriterien an Werte angelegt werden, um deren Schutzbedarf zu bestimmen. Ein weiterer Vorteil ist der, dass dadurch ein gewisser Ankerpunkt zum täglichen Geschäft der Zielgruppe gelegt und der Grad an Abstraktion des Dokuments etwas gelockert wird.
- **Grundlegende und richtungsweisende Standards:** Je nach Unternehmenszweck und Grundlage der Arbeit der IT-Security-Organisation können die verschiedensten externen Vorgaben eine Grundlage für den Schutz von Informationen darstellen. Neben den üblichen Normen kann es sich auch um gesetzliche und kundengetriebene Anforderungen handeln.
- **IT-Security-Organisation:** Die Beschreibung, wie die IT-Security-Organisation innerhalb des Unternehmens aufgestellt ist, ist von Vorteil. Zum einen wird damit von höchster Stelle aus kommuniziert, wer für diese Aufgaben verantwortlich zeichnet, und damit wird die Art Rückendeckung gegeben, die für die Umsetzung auch unangenehmer Aufgaben erforderlich ist. Werden Vorgaben formuliert, dann ist es auch wichtig, die Konsequenzen aus Fehlverhalten zu definieren. Aus diesem Grund ist es sinnvoll, aufzuzeigen, dass die Einhaltung des Regelwerks kontrolliert wird. Die dafür zuständige Stelle kann der Information Security Officer oder eine andere Stelle im Unternehmen sein.
- **Verantwortung von Mitarbeitern:** Die Art des Umgangs mit Informationen durch jeden Einzelnen definiert in entscheidender Weise das allgemeine Sicherheitsniveau. Neben entsprechenden Artikeln im Arbeitsvertrag und



laufend stattfindenden Schulungen ist die Darstellung der persönlichen Verantwortung in der Sicherheitsrichtlinie ein weiterer wichtiger Schritt zu mehr Awareness. Begriffe wie »der Besitzer von Daten« (*data owner*) können an dieser Stelle eingeführt werden.

Die kurze prägnante Ausführung der Sicherheitsrichtlinie hat einige Vorteile, führt aber auch dazu, dass wesentliche Punkte in weitere Dokumente ausgelagert werden müssen. Zu diesen Themenbereichen zählen die folgenden:

- Die Eingliederung eines IT-Risikomanagements in den Kontext des Unternehmensrisikomanagements ist ein weiterer wichtiger Punkt. Als Grundlage dazu kann unter anderen das Dokument ISO 27005 herangezogen werden. Inhalt des Dokuments ist vor allem der allgemeine Ablauf und die Verantwortlichkeiten für die einzelnen Abschnitte einer Risikountersuchung. An dieser Stelle können die Rolle des Dateneigentümers und seine Verantwortung beschrieben werden, um die Abgrenzung zwischen der IT, die Daten verarbeitet, und den Anwendern, die Daten erzeugen und ändern, näher zu beschreiben.
- Das ISMS, das in der Sicherheitsrichtlinie bereits erwähnt wurde, kann nur auf sicheren Pfeilern stehen, wenn die entsprechenden Gremien und Organisationseinheiten genannt sind, die dieses im Rahmen ihrer Aufgabe regelmäßig auditieren und pflegen. Dazu gehören auch die Zeitintervalle und der jeweilige Umfang der Tätigkeiten.
- Die Durchführung von Maßnahmen zum Schutz von Informationen oder physischen Werten folgt häufig nicht nur internen Vorgaben, sondern auch Anforderungen von außen. So wird ein Rüstungsunternehmen völlig anderen Zwängen zur Compliance ausgesetzt sein als ein Bekleidungsunternehmen. Diese Vorgaben und die Auswirkungen auf den Business-Continuity-Plan sollten kurz beschrieben werden. Diese geben den Rahmen für unternehmerisches Handeln und die Fixpunkte für Maßnahmen vor.

4.7.2 Klassifizierungsrichtlinie

Alle Aktionen, die aus Gründen der Informationssicherheit ergriffen werden, müssen zwischen den entstehenden Kosten und dem Nutzen, den die eingebrachten Maßnahmen voraussichtlich bringen, abgewogen werden. Ein wichtiger Faktor, den man dazu bestimmen muss, bevor man agiert, ist der Wert, den ein zu schützendes Objekt für das Unternehmen hat. Der Schutz des Speiseplans im Intranet ist nicht so dringend wie der Schutz von Entwick-



KAPITEL 4 – ORGANISATION VON RICHTLINIEN

lungsdaten. In diesem Fall ist es offensichtlich. Liegt der Fall aber nicht so klar auf der Hand, ist er von subjektiven Einschätzungen abhängig oder einfach nur von verschiedenen Perspektiven aus gesehen unterschiedlich bewertbar, dann ist es nötig, ein Vorgehenskonzept parat zu haben, das den Vorgang dieser Einschätzung unterstützt.

Wichtig

Der Schutzbedarf eines Unternehmenswerts bemisst sich aus den Kosten, die bei Verlust von Vertraulichkeit, Verfügbarkeit oder Integrität entstehen würden.

4

Die Klassifizierungsrichtlinie gibt Hilfestellung bei der Einschätzung eines Unternehmenswerts. Die Einklassifizierung erfolgt nach definierten Schutzzielen, die jeweils in verschiedene Schutzstufen untergliedert sind. Einfacher: Man wählt ein Schutzziel wie z.B. die Vertraulichkeit und stuft einen Unternehmenswert auf einer Skala ein. Die Gestaltung dieser Skala bleibt dabei dem Unternehmen überlassen. Ausprägungen, die häufig zu finden sind, wären vier Stufen: von eins bis vier. Stufe eins würde dabei den geringsten Schutzbedarf festlegen und Stufe vier den höchsten.



Abbildung 4.5: Einleitung einer Klassifizierungsrichtlinie

Die Wahl einer Schutzstufe muss, wird sie von verschiedenen Personen vorgenommen, möglichst immer den gleichen Wert ergeben. Aus diesem Grund muss jede Stufe in einer Form beschrieben werden, bei der es zum einen eindeutige Kriterien gibt, auf der anderen Seite aber muss sie so offen sein, dass sie für jede Art Unternehmenswert Anwendung finden kann.



VERSCHIEDENE RICHTLINIEN

4

Die Grundlage der meisten Bewertungsmatrizen ist der finanzielle Schaden, der anfallen würde, falls Informationen verloren gingen. Das führt dazu, dass Schadensklassen wie »Imageschaden« schwer einzuschätzen sind. Wie hoch ist der finanzielle Schaden, falls es öffentlich werden würde, dass Kundendaten verloren gegangen sind? Die Kosten aufgrund von vertraglichen Regelungen dagegen wären in diesem Fall einfach durch einen Juristen zu beantworten.

	Vertraulichkeit (Verlust von Informationen)	Verfügbarkeit (Informationen können nicht zur Verfügung gestellt werden, IT-Systeme stehen nicht zur Verfügung)	Integrität (Korrekturaufwand)
1 Finanzieller Schaden gering	Allgemeine Informationen Adressaten sind alle Mitarbeiter des Unternehmens.	Prozesse sind gestört, Teilaufgaben können bearbeitet werden. Geschäftskritische Prozesse sind nicht beeinträchtigt.	Daten können weiter genutzt, bzw. mit geringem Aufwand berichtet werden
2 Finanzieller Schaden mittel	Vertrauliche Informationen Adressaten sind ein eingeschränkter Personenkreis. Z. B. Projektmitglieder, Mitglieder der Abteilung.	Prozesse sind gestört, Teilaufgaben können nur unter erhöhtem Aufwand bearbeitet werden. Geschäftskritische Prozesse sind teilweise nicht verfügbar.	Daten können teilweise genutzt werden, bzw. mit erhöhtem Aufwand berichtet werden.
3 Finanzieller Schaden groß	Geheime Informationen Adressaten sind einzelne, benannte Personen. Z. B. Abteilungsleiter, Projektleiter, Vertreter des Kunden.	Prozesse sind nicht verfügbar. Teilaufgaben können nicht bearbeitet werden. Geschäftskritische Prozesse sind nur unter stark erhöhtem Aufwand verfügbar.	Daten sind unbrauchbar und können nicht korrigiert werden.
4 Finanzieller Schaden existentiell	Steng geheime Informationen Adressaten sind üblicherweise durch die Unternehmensleitung benannte Personen. Z. B. Unternehmensstrategien, strategische Produktinnovationen.	Geschäftskritische Prozesse können nicht ausgeführt werden. Ersatzprozesse sind nicht verfügbar.	Geschäftskritische Daten sind unbrauchbar und können nicht korrigiert werden.

Abbildung 4.6: Beispielhaftes Bewertungsschema einer Klassifizierungsrichtlinie

Trotz dieser Problematik hat es sich weitgehend durchgesetzt, diese Art von Bewertungsgrundlage zu nutzen. In Abbildung 4.6 ist eine Bewertungsmatrix abgebildet. Insgesamt werden darin drei Schutzziele abgebildet, aber es wäre kein großer Aufwand, weitere hinzuzufügen. Außerdem wurden vier Schutzstufen gewählt. Gründe dafür sind, dass eine gerade Zahl nicht so stark



dazu verführt, den mittleren Wert zu wählen, wie es bei drei Stufen häufig der Fall ist. Außerdem wird eine vierstufige Staffelung auch in den entsprechenden Normen wie der ISO 15504 bevorzugt.

Auffällig ist, dass in der abgebildeten Matrix der Datenschutz nicht betrachtet wird. Aufgrund der Bestimmungen der EU-DSGVO müssen bestimmte Arten von personenbezogenen Daten, unabhängig vom finanziellen Schaden, der bei Verlust entstehen würde, besonders geschützt werden. Diese Tatsache abzubilden, stellt eine Herausforderung dar. Aus der Erfahrung ist zu sagen, dass es nicht sinnvoll ist, einfach eine zusätzliche Schutzstufe einzuführen. Damit werden zum einen die Bewertungsgrundlagen »Datenschutz« und »finanzialer Schaden« vermischt, und zum anderen würde man sich damit auf eine ausschließlich in Deutschland gültige Matrix verständigen. Sinnvoller ist es, bei der Klassifizierung von Daten zunächst eine Bewertung aufgrund der Schadenshöhe vorzunehmen und zusätzlich, z.B. durch Ankreuzen, festzustellen, dass es sich beim zugrunde gelegten Unternehmenswert um personenbezogene Daten handelt. Wird die Bewertung in Form eines elektronischen Formulars vorgenommen, kann der dadurch angestoßene Workflow die Bewertung direkt in die weitere Vorgehensweise integrieren und auch den Datenschutzbeauftragten mit einbinden.

4.7.3 ISMS-Handbuch

Die Sicherheitsrichtlinie definiert den Top-down-Ansatz bezüglich der Informationssicherheit. Darin wird beschrieben, wie sich das Unternehmen diesbezüglich aufstellt, wer welche Aufgaben wahrnimmt und warum es wichtig ist, diese zu verfolgen. Die Klassifizierungsrichtlinie hält fest, dass nicht alle Vermögenswerte gleich wichtig sind. Diejenigen, die wichtiger sind, sei es aus monetärer Perspektive oder aus Sicht des Datenschutzes, müssen auch besser geschützt werden. Um diesen Vorgang formal und professionell umsetzen zu können, einigt man sich in dieser Richtlinie auf allgemeingültige Kennzahlen, die sich in Schutzzielen und Schutzklassen ausdrücken.

Das ISMS-Handbuch wiederum bildet den Leim um alle diese recht komplexen Vorgaben, indem es die Erklärungen nachliefert, wie das alles zu verstehen ist und wie die Zahnräder ineinander greifen, und zwar auf einem Niveau, das jeder Betroffene, sei er aus der IT oder aus der Produktion, auch verstehen kann. Es existiert kein festgelegter Begriff, wie dieses Dokument heißen muss. An dieser Stelle nennen wir es »Handbuch«, da es genau diese



Funktion hat, und setzen den Begriff »ISMS« davor, da es im Grunde den Gesamtkomplex des Information-Security-Management-Systems des betroffenen Unternehmens erläutert. Dieses Dokument ist üblicherweise noch individueller gestaltet als die bislang aufgeführten Richtlinien, da es bereits existierende Unternehmensfunktionen, wie das Risikomanagement oder das Compliance-Management, mit dem IT-Sicherheitsmanagement zusammenführt, und das ist in den meisten Fällen bereits über Jahre hinweg mit den Unternehmensprozessen verwachsen. Nachfolgend werden typische Themen kurz aufgeführt:

- Das **Sicherheitsleitbild**, auf Englisch das »Mission Statement«, des Unternehmens beschreibt plakativ, warum ein Unternehmen ein IT-Sicherheitsmanagement einführt und welchen Prinzipien es gehorcht. Es ist sinnvoll, an dieser Stelle bereits Ziele generisch aufzuführen und damit eine Abgrenzung zu anderen Unternehmensfunktionen zu erreichen. Dazu kann z.B. der Schutz der eigenen Vermögenswerte und der Werte von Kunden gegen externe Angreifer gehören, aber auch ein Hinweis darauf, dass gesetzliche Anforderungen an dieser Stelle wahrgenommen werden.
- Das von der Unternehmensleitung angestrebte **Schutzniveau** kann im Handbuch durchaus detaillierter aufgezeigt werden.
- Alle Stellen, die sich mit dem Schutz der Unternehmenswerte beschäftigen, werden beschrieben und das Zusammenspiel zwischen den Funktionen dargestellt. Es muss jedem Mitarbeiter auf einen Blick klar werden, was er den Datenschutzbeauftragten fragen muss und was den Manager IT-Security.
- Der Umgang mit Vermögenswerten hängt von der Einklassifizierung auf Basis der Klassifizierungsrichtlinie ab. Im ISMS-Handbuch ist der richtige Ort, um das Thema »Klassifizierung« im Detail zu beschreiben, die verschiedenen Schutzziele zu definieren, die zugrunde liegenden Prinzipien, wie das Maximumprinzip, aufzuführen und den Zusammenhang von Vermögenswerten, deren Einstufung und den abgeleiteten Maßnahmen aufzuzeigen. Dient eine Business-Impact-Analyse generell als Werkzeug, um diesen Prozess zu unterstützen, dann kann dieser Prozess zudem beschrieben werden.
- Im ISMS-Handbuch werden des Öfteren generelle Vorgaben, die einen starken Bezug zur Informationssicherheit haben, explizit festgeschrieben. Dazu kann z.B. der Umgang mit Public Clouds gehören oder aber auch der



Umgang mit Mail oder Internet. Das macht natürlich nur auf einer sehr niedrigen Detailtiefe Sinn, da die häufiger geänderten Richtlinien an einer anderen Stelle in der Richtlinienhierarchie stehen.

- Ein Kapitel sollte die wichtigsten, für jeden Mitarbeiter relevanten Sicherheitsprozesse beschreiben. Dabei kann es sich um profane Dinge wie das Zurücksetzen eines Passworts handeln oder aber um spezielle Themen wie den Objektschutz oder den Prototypenschutz. Alle vorherigen Punkte beschreiben Teilbereiche des ISMS. Was bislang noch nicht aufgeführt wurde, kann nun noch beschrieben werden. Dazu gehören häufig Punkte wie die Beschreibung der Richtlinienstruktur, die Grundsätze des Aufbaus und der Lenkung von Dokumenten, Kennzahlen bezüglich des ISMS, die Beschreibung wann welche Überprüfung zu erfolgen hat, eine Beschreibung, des Risikomanagements und manchmal auch ein Zeitplan zur Einführung einer zertifizierungsfähigen Organisation.

4

Das ISMS-Handbuch dient jedem neuen Mitarbeiter als Leitfaden, wenn es um den korrekten Umgang mit Vermögenswerten generell und Daten im Speziellen geht. Von hier aus wird er weitergeleitet zu den detaillierteren Richtlinien oder auch zu den konkreten Ansprechpartnern.

4.7.4 Richtlinie zum IT-Risikomanagement

Üblicherweise wird das IT-Risikomanagement vom Unternehmensrisikomanagement des Unternehmens abgeleitet. Ebenso verhält es sich mit der Richtlinie zum IT-Risikomanagement. Ist bereits auf Unternehmensebene ein Dokument vorhanden, so sollte dieses vorliegen, bevor man sich auf die Entwicklung einer eigenen Vorgehensweise für das IT-Risikomanagement konzentriert.

Tipp

Das IT-Risikomanagement ist in vielfältiger Form die Grundlage für eine ganze Reihe von Methoden im Rahmen des IT-Security-Managements, und schon aus diesem Grund ist es sinnvoll, dafür definierte Rahmenbedingungen vorzugeben.

Als Top-Level-Dokument ist auch diese Richtlinie an alle Mitarbeiter gerichtet und soll auch von allen genutzt werden. So hat jeder Ersteller sensibler



Daten die Verpflichtung, diese Daten zu klassifizieren und entsprechend der Einstufung damit umzugehen. Die Klassifizierung, also die Bewertung der Wichtigkeit der Daten, ist bereits Teil des Risikomanagements und basiert auf der Klassifizierungsrichtlinie. Für die Quantifizierung eines Risikos sind weitere Attribute zu bewerten. Dazu gehören die Faktoren »Bedrohung« und »Eintrittswahrscheinlichkeit«. Die Richtlinie zum IT-Risikomanagement beschreibt unter anderem, wie diese Bewertung vorgenommen werden soll.

Da nicht jeder Mitarbeiter mit der Thematik der Risikobewertung vertraut ist, muss die Richtlinie allgemein und doch praxisnah gehalten werden. Bereiche, die eine Richtlinie zum IT-Risikomanagement enthalten kann, sind:

- Einordnung in den Unternehmenskontext und Zusammenhang mit den Vorgaben des Unternehmensrisikomanagements
- Hinweise auf die Wichtigkeit, den Umgang mit Daten und IT-Systemen anhand einer Risikoüberprüfung zu steuern. Der Zusammenhang zwischen Risiko und Vorgehensweise bei der Ergreifung von Maßnahmen sollte dargestellt werden.
- Anhand von Beispielen sollten der Vorgang des IT-Risikomanagements und die Ableitung entsprechender Maßnahmen erklärt werden. Der Prozess sollte dabei so allgemeingültig dargestellt werden, dass dadurch alle relevanten Fragestellungen abgedeckt werden.
- Eine Liste maßgeblicher Bedrohungen kann dem Mitarbeiter helfen, seine individuelle Problematik besser einzuordnen.
- Eine Liste mit den Unternehmenswerten wie Daten, IT-Systemen, Zugangsrechten oder Applikationen, die einem IT-Risikomanagement unterzogen werden können, kann als Anhalts- und Ausgangspunkt bereitgestellt werden.
- Interne und externe Anforderungen an die IT-Security: gesetzliche Anforderungen oder vertragliche Verpflichtungen gegenüber Kunden und Lieferanten. So kann es vertragliche Verpflichtungen geben, dass Prototypen eines Kunden grundsätzlich mit einer sehr hohen Sicherheitseinstufung zu versehen sind und dass damit bestimmte Maßnahmen in jedem Fall getroffen werden müssen. Diese Einschätzung kann abweichen von der, die der damit betreute Sachbearbeiter normalerweise vergeben würde.
- Eine Liste mit Ansprechpartnern im Unternehmen



4.7.5 IT-Sicherheitsrichtlinie

Die IT-Sicherheitsrichtlinie, auch als »IT-Security Policy« bezeichnet, adressiert nicht mehr alle Mitarbeiter, sondern fokussiert sich auf die Mitarbeiter der IT-Abteilung. Damit hat sie nichts mehr mit der allgemeinen Sicherheitsrichtlinie gemeinsam. Anstelle allgemeiner Aussagen über Wichtigkeit und Zweck von IT-Security wird in der IT-Sicherheitsrichtlinie über Maßnahmenziele zu IT-Themen geschrieben.

Als Dokument der zweiten Ebene handelt es sich aber nicht um ein Handbuch mit technischen Details für Administratoren. Vielmehr bildet es alle Themen der IT-Security ab, definiert deren Bearbeitung und verweist dann gegebenenfalls auf die Arbeitsdokumente der dritten Ebene. So wird in der IT-Sicherheitsrichtlinie unter dem Oberbegriff »Netzwerk« stehen, dass Zugänge zum Wireless-Netzwerk (WLAN) abgesichert sein müssen, dass dies unter der Nutzung von Zertifikaten zu geschehen hat, dass eine Dokumentation vorliegen muss und dass regelmäßige Überprüfungen vorgeschrieben sind. Wie aber ein Administrator die bei ihm vor Ort eingesetzte Hardware konfigurieren muss, das findet er dann in der WLAN-Richtlinie, einem Dokument der dritten Ebene.

Warum die Trennung von übergeordneter IT-Sicherheitsrichtlinie und administrativen Anleitungen? In kleinen Unternehmen kann man sehr gut beide Ebenen in einem Dokument zusammenfassen. Auch wenn es dabei sehr umfangreich werden kann, ist die Pflege doch noch machbar. Für ein großes Unternehmen mit vielen IT-Mitarbeitern ist die Pflege in einem Dokument unhandlich und fehleranfällig. Dazu kommen die unterschiedlichen Wartungsintervalle. Die IT-Sicherheitsrichtlinie mit nicht-technischen Inhalten muss nicht so häufig angepasst werden wie hard- und softwarenahe Anleitungen.

Die Struktur der IT-Sicherheitsrichtlinie kann auf unterschiedliche Weise gestaltet werden. Aus diesem Grund reicht die Darstellung von frei formulierten Texten bis hin zu tabellarisch angeordneten Themen. Die zweite Variante führt zu einem deutlich übersichtlicheren Dokument, in dem Änderungen auch sehr viel einfacher durchgeführt und kenntlich gemacht werden können.

Unterschiedliche Normungsorganisationen bieten Gliederungen für eine IT-Sicherheitsrichtlinie unter den verschiedensten Namen an. Neben den Dokumenten des BSI gehört vor allem auch das ISO-27002-Dokument dazu. Im Grunde kann dessen Aufbau als Grundgerüst für eine eigene Richtlinie he-



rangezogen werden. Neuere Themen bzw. Themen, die aufgrund der Art des Geschäftsbetriebs auftreten und nicht in der ISO 27002 abgebildet sind, können problemlos angefügt werden.

Die Gliederung einer IT-Sicherheitsrichtlinie ohne diese eben erwähnten Teilaspekte könnte wie folgt aufgebaut sein:

- **Metadaten:** Dazu gehören der Name des Dokuments, die Version, die Stelle, die die Richtlinie abgenommen hat, und das Datum.
- **Einführung:** Das erste Kapitel kann genutzt werden, die Thematik der Informationssicherheit zu erläutern. Was bedeutet es für das Unternehmen und für jeden einzelnen Mitarbeiter, warum wird es benötigt und wie können diese Richtlinien helfen, Informationssicherheit zu etablieren? Häufig wird an dieser Stelle auch die Gesamtstruktur aller Richtlinien im Bereich der Informationssicherheit aufgezeigt. Dazu gehören alle Richtlinien und alle weiteren Quellen, in denen Vorgaben gemacht und Sachverhalte zur Informationssicherheit abgelegt sind.
- **Geltungsbereich:** Wie für alle anderen Richtlinien gilt auch hier der Grundsatz, dass der Wirkungsbereich des Dokuments klar definiert sein muss.
- **Abkürzungen und Erläuterungen:** Auch wenn viele Fachtermini der Informatik die breite Öffentlichkeit erreicht haben, so ist es dennoch nützlich, dass Begriffe und vor allem Abkürzungen kurz vorgestellt werden, bevor sie in der Richtlinie verwendet werden.
- **Informationssicherheitsorganisation:** Es ist eine der grundlegenden Anforderungen an ein IT-Security-Management, die Informationssicherheit in die Organisationsstruktur einzubauen. Dazu gehört auch die Beschreibung ihrer Kompetenzen, des Wirkungsbereichs und der Aufgaben. In welcher Weise Sicherheitsprobleme an diese Organisation zu melden sind und welche Wege und Vorgehensweise dafür einzuhalten sind, ist Bestandteil dieses Kapitels. Die internen Manager IT-Security sind in ständigem Kontakt mit anderen internen und externen Stellen. Dazu gehören vor allem der Datenschutzbeauftragte, die Personalabteilung und die IT. Der regelmäßige Informationsaustausch mit diesen Stellen ist essenziell.
- **Umgang mit Informationen und informationsverarbeitenden Systemen:** Am Anfang jeder Anleitung zum Umgang mit Systemen stehen die Beinstellungsaufnahme und nachfolgend die Verwaltung von IT-Systemen und



von Informationen. Nur wenn man weiß, wo Daten anfallen, kann man auch definieren, wie damit umzugehen ist. Dazu gehört auch jeweils die Pflege von Attributen wie z.B. des Data Owners bzw. des Risk Owners. Der Umgang mit Daten wird in der Sicherheitsrichtlinie angerissen und deren Bewertung dann in den Dokumenten zum Risikomanagement und zur Klassifizierung beschrieben. In der IT-Sicherheitsrichtlinie sollte schlussendlich der Bezug zur täglichen Arbeit eines jeden Mitarbeiters hergestellt werden.

- **Sicherheit im Personalmanagement:** Wie geht das Unternehmen mit Zugriffs- und Zugangsrechten um? Wie sehen die Abläufe aus, die einer Vergabe von Zugriffsrechten vorgeschaltet sind, wie das Change-Management während der Anstellung, und wie sehen die Prozesse aus, wenn ein Mitarbeiter das Unternehmen verlässt? Diese Fragen beantwortet das Kapitel »Personalmanagement«. Dazu kommen Regelungen für den Umgang mit externen Mitarbeitern, mit Praktikanten oder Diplomanden und mit Kollegen aus verbundenen Unternehmen wie z.B. Joint Ventures.
- **Physische Sicherheit:** Der Bereich der »physischen Sicherheit« umfasst eine große Bandbreite an Regelungen. Es beginnt bei den Zutrittsregeln zum Unternehmenscampus selbst und zu sensiblen Bereichen wie dem Rechenzentrum oder der IT-Abteilung und endet beim Schutz von einzelnen IT-Systemen oder Devices vor Diebstahl oder Sabotage. Dabei werden alle Stadien abgedeckt, die eine Hardware durchläuft: von der Anlieferung über den Aufbau bis hin zum Abbau und der Entsorgung. Regelungen zur fachgerechten Entsorgung von Festplatten und Papier in Ordnern können also auch in diesem Kapitel behandelt werden.
- **Umgang mit IT-Equipment:** Wird im Kapitel »Physische Sicherheit« der Fokus auf die Hardware selbst gelegt, so werden in diesem Kapitel auch die Bedienseite und die auf Gerätschaften abgelegten Daten thematisiert. Dazu gehören der Umgang mit Kameras, Wechselmedien, das Brennen von DVDs oder das Mitbringen von privaten Gerätschaften genauso wie der Umgang mit Internet, E-Mail und Daten im Allgemeinen. Der Komplex »bring your own device« (BYOD) kann an dieser Stelle oder aber in einem weiteren Dokument abgehandelt werden. Es handelt sich dabei um eine Unternehmensstrategie mit dem Ziel, dass Mitarbeiter jede Art von Gerätschaft mitbringen können. Die zuständigen IT-Abteilungen haben dann die Aufgabe, diese Geräte, zumeist Mobiltelefone und Ähnliches,



- mit in das Unternehmensnetzwerk einzubinden. Die damit verbundenen Risiken müssen durch erhöhten technischen Aufwand wieder begrenzt werden.
- **Zugriffskontrolle:** Jeder darf nur auf die Informationen Zugriff erhalten, die er für die Erledigung der ihm zugewiesenen Aufgabe benötigt. Dieser Grundsatz liegt den Regelungen zum Zugriffsschutz zugrunde. Dazu kommen erweiterte Maßnahmenziele wie das Vieraugenprinzip, um sensible Daten gezielt zu schützen. Im Kapitel »Personalmanagement« werden die Prozesse beschrieben, die ablaufen, um Berechtigungen einzurichten, zu ändern und am Schluss des Arbeitsverhältnisses zu entziehen. In diesem Kapitel werden die technischen Details definiert. Dazu gehören die Regelungen für Passwörter, spezielle Benutzerrechte für Administratoren und für Systembenutzer, die Authentifizierung im Allgemeinen, die Protokollierung von Zugriffen oder von Anmeldedetails, Softwaresicherheit und Sicherheit bei anderen Devices wie z.B. Telefonen oder Faxgeräten. Der Bereich Verschlüsselung ist ein weiterer Aspekt, der dazu dient, den Zugriff auf Daten nur durch dazu befugte Personen zu gestatten.
 - **Operatives Management:** In diesem Kapitel werden alle Maßnahmenziele und Dokumente aufgeführt, die den Betrieb und die Aufrechterhaltung des IT-Betriebs definieren. Dazu gehören das Change-Management, der Support und die Administration von IT-Systemen. Dabei ist es ohne Belang, ob es sich um externe oder interne Mitarbeiter handelt, die diese Aufgaben wahrnehmen. Jedes IT-System bzw. der Service, der dahintersteckt, hat einen Lifecycle. Dieser beginnt bei der Anforderung, geht über die Planung und die Inbetriebnahme bis hin zur Pflege. Alle diese Schritte gehören unter den verschiedenen Aspekten des Informationsschutzes durchleuchtet und beschrieben. Dabei bedeutet Service die volle Bandbreite an IT-Dienstleistungen. Wichtiger Bestandteil sind die Beziehungen zu Lieferanten, von denen IT-Systeme bezogen werden, und die Verträge bezüglich Support und Wartung dieser Gerätschaften.
 - **Compliance:** Die Aufführung von weiteren Maßnahmenzielen, die auf der Basis von gesetzlichen oder normativen Vorgaben basieren, ist Bestandteil dieses Kapitels. Vor allem interne Richtlinien können an dieser Stelle aufgeführt werden, um den größeren Zusammenhang aufzuzeigen.



4.7.6 IT-Systemrichtlinien

Die Verwaltung von IT-Systemen in heterogenen Umgebungen setzt ein großes Maß an Wissen bei den betreuenden Fachspezialisten voraus. Trotzdem wird es aufgrund sich laufend ändernder Soft- und Hardware beinahe unmöglich, alle Prozeduren, die zum Betrieb erforderlich sind, im Kopf zu behalten. Dazu kommen Bestrebungen nach Standardisierung und Überprüfbarkeit der IT-Infrastruktur. Auch der Bereich der Sicherheitsanforderungen erfordert großes Detailwissen von allen Beteiligten. Um diesen Anforderungen gerecht werden zu können, ist es erforderlich, idealerweise für jedes einzelne kritische IT-System eigene Systemrichtlinien zu erstellen. Die Bandbreite des Inhalts kann sich dabei von vollständigen Installations- und Konfigurationshandbüchern bis hin zu reinen Anleitungen zur Härtung der entsprechenden Systeme erstrecken. Was abgedeckt werden soll, hängt maßgeblich davon ab, wie ein Unternehmen aufgestellt ist und ob ein System als kritisch eingestuft wird.

Werden die Aufgaben Aufbau von Hardware, Installation Grundsysteum und Installation Software von verschiedenen Bereichen innerhalb des Unternehmens wahrgenommen, so ist es durchaus sinnvoll, für jeden Bereich individuelle Vorgaben bereitzustellen. Je mehr dieser Aufgaben aber von nur einem oder zwei Bereichen wahrgenommen werden, so kann durchaus auch nur eine einzelne IT-Systemrichtlinie bestehen.

Die IT-Systemrichtlinie stellt eine konkrete Handlungsanweisung für ein definiertes IT-System dar. Dies ist nicht für alle IT-Systeme erforderlich, und oft kann auf die übergeordnete IT-Sicherheitsrichtlinie verwiesen werden. Der Übergang zwischen den beiden Richtlinien ist damit fließend. Ist die IT-Sicherheitsrichtlinie eher abstrakt gehalten und für ein großes Publikum gedacht, so ist die IT-Systemrichtlinie eher technisch geprägt und detailliert ausgeführt. Zielgruppe sind hier die Experten der verschiedenen Disziplinen.

Entsprechend dem Detaillierungsgrad ist auch der Umfang einer solchen IT-Systemrichtlinie im Allgemeinen recht groß und häufigeren Änderungen unterworfen. Im Rhythmus von Softwareupdates und Hardwareveränderungen müssen häufig Inhalte angepasst werden. Es müssen deshalb Verantwortliche definiert werden, die solche Wartungen an den Richtlinien planen und nachvollziehbar umsetzen.

Der Aufwand, der für die Erstellung und Pflege von IT-Systemrichtlinien getrieben werden muss, ist nicht zu unterschätzen. Aus diesem Grund sollten



Entscheidungskriterien definiert werden, nach denen entschieden wird, ob für ein bestimmtes IT-System eine IT-Systemrichtlinie aufgesetzt wird oder ob dies nicht erforderlich ist. Aus Unternehmenssicht wird dies häufig an dem möglichen Schaden festgemacht, den der Ausfall des Systems verursachen würde. Basis dafür ist die Annahme, dass eine solche IT-Systemrichtlinie häufig Teil eines IT-Business-Continuity-Plans darstellen wird. Aus Sicht der Informationssicherheit ist es wichtig, dass Systeme standardisiert und aktualisiert werden und damit auf Basis einer IT-Systemrichtlinie aufgebaut sind, die Daten verarbeiten, die als kritisch klassifiziert werden. Damit soll erreicht werden, dass Systeme, die aus der Sicherheitsbrille heraus gesehen als wichtig eingestuft werden, einem kommunizierten Standard entsprechen. In großen Unternehmen werden solche Systeme oft in mehreren Standorten eingesetzt, und dem Manager IT-Security wird es schwerfallen, eine Sicherheitseinstufung vorzunehmen, wenn diese Systeme unterschiedlich ausgeführt sind, obwohl alle die gleichen Aufgaben haben.

4

4.8 Von der Theorie in die Praxis

Richtlinien werden von Fachleuten erstellt und spiegeln die Erfordernisse wider, die sie in Zusammenhang mit ihrem Aufgabengebiet sehen. So sieht eine Richtlinie zum Gebrauch von E-Mail anders aus, wenn sie der Manager IT-Security erstellt, als wenn dies durch den Administrator des E-Mail-Systems geschieht.

Der Letzte in der Kette ist der Benutzer, der die Richtlinie letzten Endes »leben« soll. Erleichtert sie sein Arbeitsleben, dann stellt dies im Allgemeinen kein großes Problem dar. Macht es seine Arbeit komplizierter, dann sind einige Methoden der Kommunikation erforderlich, um die Durchsetzung trotzdem zu erreichen. Dabei ist immer zu bedenken, dass die eben beschriebene Richtlinie ja nur eine einzelne in einem unüberschaubaren Pool an ähnlichen Richtlinien darstellt.

Tipp

Richtlinien sind Anweisungen und sollten deshalb auch von den jeweiligen Leitungsebenen vorgegeben werden. Der Vorgesetzte sollte sie kommunizieren und vorleben. Alternativ kann es bereits ausreichen, wenn



KAPITEL 4 – ORGANISATION VON RICHTLINIEN

das Deckblatt zur Richtlinie ein »Abgenommen und angewiesen durch« enthält, inklusive des Namens des Vorgesetzten oder der Rolle. Dadurch gewinnt sie an Verbindlichkeit.

Existiert die Richtlinie, dann muss sie kommuniziert werden. Sie auf einen Datenserver zu stellen und eine E-Mail mit der Bitte zu verschicken, regelmäßig dort vorbeizuschauen und die neuen Regelungen zu verinnerlichen, reicht dabei nicht aus. Kommunikation bedeutet, dass jeder betroffene Mitarbeiter mit der jeweiligen Richtlinie direkt in Kontakt gebracht werden muss. Das kann in Form der eben erwähnten E-Mail geschehen, nur die Sprachregelung müsste modifiziert werden.

4

»Herr Müller, eine neue Richtlinie zur Thematik Internetnutzung wurde im Intranet unter der Adresse ... veröffentlicht. Ich bitte um Beachtung und Umsetzung der dort aufgeführten Regeln. Bei Fragen wenden Sie sich bitte umgehend an folgende Stelle:...«

Diese E-Mail vom Vorgesetzten stellt eine Anweisung dar und enthält alle Informationen, die der Mitarbeiter benötigt.

Hat ein Mitarbeiter eine neue Richtlinie erhalten und hat er verstanden, dass sie umzusetzen ist, dann muss ihm auch die Möglichkeit gegeben werden, dies zu tun. Daraus ergeben sich zwei weitere Forderungen. Zum einen muss er die technischen Möglichkeiten haben, die Richtlinie gemäß der Vorgaben umzusetzen, und zum anderen muss er wissen, wie dies zu tun ist. Der erste Punkt muss erfüllt sein, bevor die Richtlinie in Kraft tritt. Der zweite Punkt muss in Form einer Schulung angeboten werden, sobald die Richtlinie veröffentlicht wurde.



5 Betrieb der IT-Security

5.1 Kapitelzusammenfassung

Um die übergeordneten betrieblichen Grundsätze eines Unternehmens erfüllen zu können, müssen im Rahmen des IT-Security-Managements eine Reihe von Prozessen installiert werden. So wird aus der Sorgfaltspflicht des Unternehmers ein Prozess zur gesteuerten Vergabe von Rechten abgeleitet. Diese Prozesse soll der Manager IT-Security reglementieren, implementieren, steuern und überwachen.

Die Top-5-Fragen zum aktuellen Kapitel:

- Existiert ein Modell, das die übergeordneten betrieblichen Grundsätze auf die Anforderungen an die IT-Security-Organisation abbildet?
- Sind Richtlinien für das Identitätsmanagement vorhanden?
- Wurden Richtlinien erstellt, die den Einsatz von IT-technischen Betriebsmitteln regeln?
- Ist der Manager IT-Security in alle Softwareentwicklungsprozesse und die Neueinführung von Kaufsoftware involviert?
- Wird die Vergabe und der Entzug von Rechten von neuen Mitarbeitern, Kollegen, die im Unternehmen die Aufgabe wechseln, und von solchen, die aus dem Unternehmen ausscheiden, durch entsprechende Vorgaben geregelt?

5.2 Einführung

Kernaufgabe der IT-Security-Organisation ist es, alle Aspekte des täglichen (IT-)Betriebs aus dem Blickwinkel der IT-Security im Auge zu behalten und gegebenenfalls auf Anpassungen hinzuwirken. Man könnte es auch so ausdrücken: Die tägliche Arbeit eines Verantwortlichen für die IT-Security besteht darin, laufend Bedrohungen und Schwachstellen hinsichtlich von Informationen zu erkennen und darauf reagierend Maßnahmen anzustossen. In anderen Fällen kann er wahrscheinlich in der Zukunft auftretende Pro-



KAPITEL 5 – BETRIEB DER IT-SECURITY

bleme im Vorfeld antizipieren und Vorsorgemaßnahmen einleiten. Themenbereiche wie das IT-Risikomanagement, das IT Business Continuity Management, die Schutzbedarfsfeststellung, das Richtlinienmanagement, technische Maßnahmen und die Konfiguration von Systemen sind die Werkzeuge, die dazu benötigt werden.

5

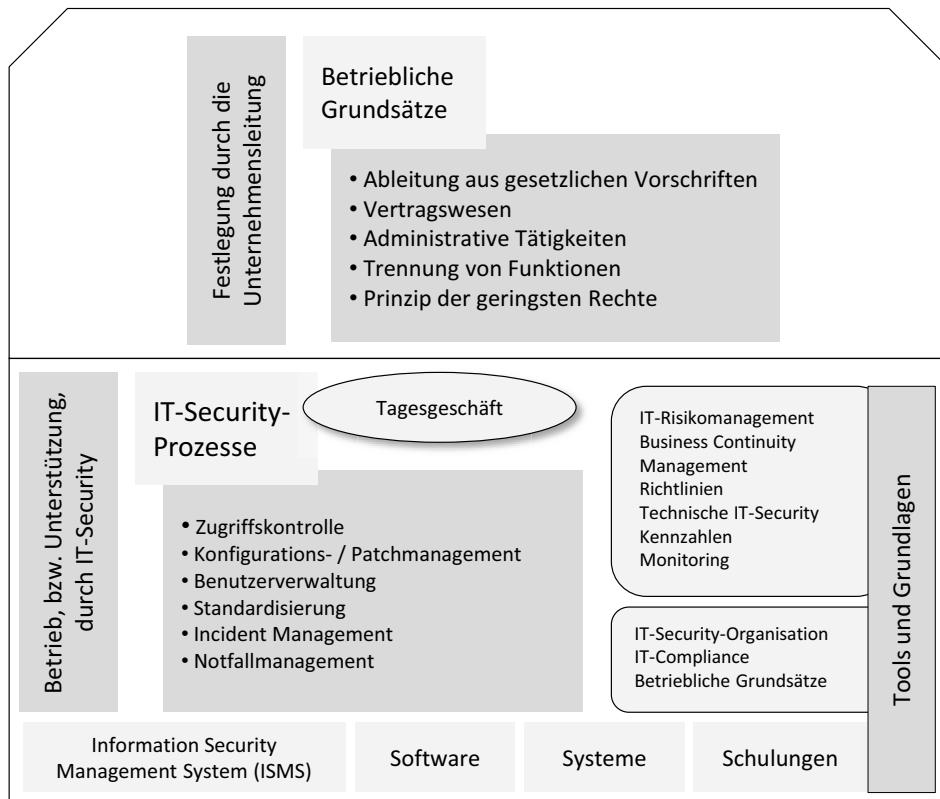


Abbildung 5.1: IT-Security-Prozesse im Unternehmen

Im Alltag stürmt täglich eine Vielzahl unterschiedlichster Anforderungen auf den Manager IT-Security ein, die zum großen Teil spontan gelöst werden müssen. Um dieser Flut an Aufgaben Herr werden zu können, muss sie kanalisiert werden, und dies ist die Aufgabe der IT-Security-Prozesse.

Entscheidende Grundlage für die Definition und den Betrieb der IT-Security-Prozesse ist ein existierendes, aktuelles Grundsatzdokument oder eine allgemein anerkannte Vereinbarung, in der die betrieblichen Grundsätze festge-



legt sind. Die betrieblichen Grundsätze legen auf Ebene der Unternehmensstrategie fest, wie mit Daten umgegangen wird und welchen Grundsätzen die Informationstechnologie im Unternehmen zu folgen hat. In Abschnitt 5.4 werden die betrieblichen Grundsätze näher erläutert.

5.3 IT-Security und der IT-Betrieb

Das IT-Security-Management steht ebenso wie die IT-Organisation im Spannungsfeld verschiedenster Anforderungen. Die IT fungiert zumeist innerhalb eines Unternehmens als Dienstleister und hat damit die Aufgabe, Services bereitzustellen, die soweit möglich standardisiert sein sollten, aber immer wieder auch individualisiert angeboten werden müssen. Jede Abweichung von der Norm macht die Kontrolle und damit auch die Sicherstellung von IT-Security schwieriger. Zu nennen sind unter vielen anderen die sogenannten VIP-Services, also die Bereitstellung von Ausnahmen vom Standard, z.B. für Mitglieder der Unternehmensleitung. Das birgt die doppelte Gefahr, dass zum einen der Betrieb dieser Services wie die allerneueste Laptop-Generation oder ein neues Mobiltelefon, zusätzliches Wissen verlangt, das häufig nicht vorhanden ist, und zum anderen, dass gerade durch diesen Personenkreis besonders sensible Daten verarbeitet werden. Ausnahmeregelungen stellen damit den Gegenpol zu verbindlichen Standards dar. Das Gleiche gilt für strikte Vorgaben wie z.B. die Nutzung von Internet und E-Mail. Gemeinsam ist in diesen Ausnahmeregelungen immer, dass der Aufwand der Kontrolle und der Sicherstellung von Datensicherheit unverhältnismäßig hoch ist. In diesen Fällen ist die Dokumentation von Ausnahmen eine erforderliche Maßnahme.

Sicherheit kostet Geld, und die Umlegung dieser Kosten auf Produktpreise ist dem Kunden im Allgemeinen schwer vermittelbar. Damit ist IT-Security ein Kostenfaktor, dessen Streichung zunächst vor allem positive Ergebnisse zeigt: nämlich die Einsparung von Geld. Auch wenn dieser Bereich heute ähnlich alternativlos gesehen wird wie das Abschließen von Versicherungen, so ist dennoch auch weiterhin ein stetiger Kampf um Budgets zu erkennen.

Weitere Gegenpole sind die Flexibilität der IT und die Einhaltung strikter Vorgaben. Es hat noch niemand behauptet, dass die Einführung eines IT-Security-Managements die Entscheidungsfindung beschleunigt und die Kosten des Betriebs senkt. Aus diesem Grund hat die IT-Security schon immer den



Nimbus des »Verzögerers« gehabt und steht mit ihren Maßnahmen nicht für einen flexiblen Betrieb mit kurzen Entscheidungsprozessen. Dass dies keine grundsätzliche Wahrheit ist, muss der Manager IT-Security in geeigneter Form nachweisen. Dazu dienen formale Prozesse, die nicht nur Sicherheit gewährleisten, sondern auch Transparenz und Standardisierung fördern. Diese beiden Faktoren wiederum wirken sich positiv auf laufende Kosten aus.

Die Digitalisierung der Unternehmen und die damit einhergehende wachsende Notwendigkeit von Agilität und neuen Methoden stellt klassische Managementsysteme der Informationssicherheit vor zusätzliche Herausforderungen. Viele eingespielte Prozesse funktionieren nicht mehr in derselben Art und Weise, wenn es statt um klassische Arbeitsplatzrechner um kommunikationsfreudige Produktionsmaschinen geht. Es ist deshalb nicht nur erforderlich, technisch immer am Ball zu bleiben, sondern auch die Fachabteilungen, mit denen es der Manager IT-Security zu tun hat, wandeln sich und müssen mit eingebunden werden.

5

5.4 Betriebliche Grundsätze

Das Betreiben eines Unternehmens folgt grundlegenden Prinzipien. Einige dieser Prinzipien lassen sich auf das IT-Security-Management übertragen. Die Rückbesinnung auf diese Grundsätze des unternehmerischen Handels ist wichtig, um eine allgemein anerkannte Basis für die IT-Security aufzuzeigen.

5.4.1 Ableitung aus gesetzlichen Vorschriften

Es gibt bis heute kein Gesetz, das die Aufgaben einer IT-Security-Organisation in einem Unternehmen konkret verbindlich macht. Die noch relativ junge EU-DSGVO kommt dem aber schon sehr nahe, denn sie legt fest, dass Mechanismen und Prozesse zur Sicherung von personenbezogenen Daten eingeführt werden müssen, die man anerkanntermaßen einer IT-Security-Organisation zuschreiben muss. Ein weiteres Beispiel, was aus Gesetzen und Vorschriften abgeleitet werden kann, ist der Zwang zur kaufmännischen Sorgfaltspflicht. Vor allem in § 43 des GmbH-Gesetzes wird dieses Erfordernis formuliert. Unter der Überschrift »Haftung der Geschäftsführer« werden die Haftung und die Pflicht zur »Sorgfalt eines ordentlichen Geschäftsman-nes« explizit genannt. Die Sorgfaltspflicht eines Unternehmers besteht in der Pflicht, Schaden vom Unternehmen fernzuhalten, und beinhaltet die Tugen-



den Umsichtigkeit, verantwortliches Handeln, Vorsichtigkeit, sorgsames und praktisches Handeln. Daraus kann abgeleitet werden, dass Informationen und Daten genauso sorgfältig zu behandeln sind wie bereits seit Langem existierende Medien wie Briefe, Akten oder Dokumente. Die Gleichstellung von Informationen in Papierform und elektronisch bedingt also die gleiche Verantwortung, wenn auch die Mittel, diese wahrzunehmen, gänzlich unterschiedlich sind.

Neben den Regelungen der genannten Gesetze können auch aus vielen anderen Gesetzen betriebliche Grundsätze abgeleitet werden, deren Umsetzung eine IT-Sicherheitsarchitektur erforderlich macht. Mehr zu diesem Thema ist im Kapitel »IT-Compliance« zu finden.

5.4.2 Vertragswesen

Verträge mit Kunden, Lieferanten oder Behörden regeln oft auch den Umgang mit Daten. In Bezug auf personenbezogene Daten sind diese Regelungen sehr konkret und detailliert im Bundesdatenschutzgesetz-Neu und der EU-DSGVO geregelt. Wenn es um sensible Daten geht, die einem Lieferanten überlassen werden, damit dieser seinen Auftrag durchführen kann, oder im umgekehrten Fall, wenn ein Lieferant oder Dienstleister Daten übermittelt, dann sollte der Umgang mit diesen vertraglich geregelt sein. Neben reinen Daten müssen auch alle anderen Werte in diese Überlegungen mit eingebracht werden. Dabei kann es sich um Prototypen, Papierdokumente, Güter oder auch Know-how handeln, das mündlich übermittelt wird. Der Umgang mit diesen Werten unterliegt wiederum der kaufmännischen Sorgfaltspflicht und in einigen Fällen auch gesetzlichen Regelungen. Alles, was nicht direkt daraus abgeleitet werden kann, sollte in eine eigene vertragliche Regelung eingebunden werden.

5.4.3 Administrative Tätigkeiten

Die Administration von IT-Systemen und Software stellt einen wesentlichen Bestandteil der Informationssicherheit innerhalb eines Unternehmens dar. Die Auswahl von Mitarbeitern für diese Aufgabe und die Festlegung der jeweiligen administrativen Bereiche ist Aufgabe des Managements. Die Haltung für eine angemessene Sicherstellung von Sicherheit in diesem Zusammenhang liegt im Rahmen der Sorgfaltspflicht wieder bei der Unternehmensleitung.



Zunächst steht die Frage im Vordergrund, wie die Sicht auf diesen Personenkreis sein soll. Im Grunde handelt es sich um die Frage, ob man den Administratoren grundsätzlich traut oder eben nicht. Abhängig von der Antwort sind im ersten Fall größere Anstrengungen zu unternehmen, was die Auswahl der Personen und deren Schulung, aber auch deren Kontrolle angeht. Dazu kommen Regeln im Umgang mit Daten wie die Trennung von Pflichten oder das Vieraugenprinzip. Im zweiten Fall müssen zusätzlich technische Maßnahmen implementiert werden, die dazu dienen, Daten zu schützen und ungewollte Änderungen an Systemen zu verhindern. Üblicherweise wird in diesem Fall ein Verschlüsselungssystem etabliert, das sicherstellt, dass nur die jeweiligen Besitzer der Daten und der Personenkreis, den sie als weitere Leser oder Mitautoren bestimmen, auf die Daten in Klarschrift zugreifen können. Da dies nur Sinn macht, wenn alle Transportmedien wie Netzwerke, E-Mail oder Datenserver in dieses System mit eingebunden sind, ist der Aufwand entsprechend groß.

In allen Fällen ist eine Kosten-Nutzung-Betrachtung sinnvoll, um für den jeweiligen Schutzbedarf ausgewogene und angemessene Maßnahmen zu finden.

Teil der Sorgfaltspflicht des Unternehmers ist es zudem, die Tätigkeiten von Administratoren zu kontrollieren. Das ergibt sich aufgrund ihrer herausgehobenen Tätigkeit und der Gefahr, die dementsprechend im Falle des Missbrauchs von ihnen ausgeht. Dazu gehört ein aktives Monitoring genauso wie die Auswertung von Protokolldaten, die Bewegungen von Datenströmen dokumentieren.

5.4.4 Trennung von Funktionen

Die Trennung von Funktionen (*separation of duties*), auch als Gewaltentrennung bezeichnet, beschreibt das Prinzip, dass für einen Vorgang mehrere Personen eingebunden werden. Für den Bestellvorgang würde das bedeuten, dass der Wareneingang und die Bestätigung im System, dass die Ware den Empfänger erreicht hat, von unterschiedlichen Stellen verantwortet werden. Erreicht werden soll dadurch, dass die Möglichkeit des Missbrauchs erschwert wird. Hinsichtlich des Vermeidens von Fehlern wird dieses Prinzip in vielen Bereichen der Informationstechnologie eingesetzt. Zu nennen ist die Softwareentwicklung, in der ein Programmierer nicht gleichzeitig auch die Qualitätsprüfung vornehmen sollte, oder allgemein der Bereich der IT-Security, in der die



Aufgaben »Implementierung von Maßnahmen« und »Kontrolle der Wirksamkeit von Maßnahmen« von unterschiedlichen Personen, besser: unterschiedlichen Bereichen, durchgeführt werden sollten.

Um die erfolgreiche Trennung von Funktionen zu überprüfen, wird im Allgemeinen die Frage gestellt: »Kann eine einzelne Person diesen Vorgang komplett durchführen, und falls ja, lässt sich diese Tatsache missbrauchen?«

In der Praxis gibt es mehrere Möglichkeiten, dieses Prinzip umzusetzen. In einem Softwaresystem werden die verschiedenen Aufgaben in Rollen zusammengefasst, die jeweils so Personen zugeordnet werden, dass der Missbrauch, wie er oben geschildert wurde, nicht stattfinden kann. Sogenannte »Governance Risk and Compliance Software« (GRC-Software) wird eingesetzt, um in komplexen Systemen auf Basis vorgefertigter Tabellen nach Verletzungen dieses Prinzips zu suchen und dies regelmäßig zu berichten. Ein solches Vorgehen kann beliebig komplex werden, was deutlich wird, wenn man sich den Grad an softwaregestützter Datenverarbeitung betrachtet, der heute üblich ist.

Daneben gibt es das Prinzip der zwei Unterschriften (*two signatures*). In diesem Fall kann eine Freigabe nur dann stattfinden, wenn sie von zwei oder mehr Personen autorisiert wurde. Dieses Vorgehen ist in Bestellvorgängen üblich. Während das Prinzip der zwei Unterschriften vor allem in sequenziell angelegten Workflows zum Tragen kommt, dient das Vieraugenprinzip dazu, einen definierten Vorgang durch mindestens zwei Mitarbeiter begleiten zu lassen. Typisch für diese Vorgehensweise sind alle Vorgänge, die einer späteren Überprüfung standhalten sollen. Dazu gehört z.B. die Auswertung von Protokolldateien, die Daten der Internet-Nutzung von Kollegen enthält, oder eine forensische Untersuchung eines Arbeitsplatzrechners.

5.4.5 Prinzip der geringsten Rechte

Das Prinzip der geringsten Rechte (*least privileges*), die erforderlich sind, dass ein Mitarbeiter seine Arbeit verrichten kann, soll sicherstellen, dass im Falle des Datenmissbrauchs ein möglichst geringer Schaden entsteht. Dieses Prinzip steht entgegen dem Prinzip übermäßiger Rechte (*excessive privileges*), das häufig in kleineren Unternehmen angewendet wird für den Fall einer spontanen Vertretung von Kollegen. Es ist anerkannt, dass dies der Sorgfaltspflicht der Unternehmensleitung widerspricht. Auch fehlendes Wissen führt in vielen Unternehmen dazu, dass viel zu viele Benutzer administrative Rechte auf



IT-Systemen haben. Die Bereinigung solcher Missstände ist aufwendig, hat aber den großen Vorteil, dass im Zuge einer solchen Überarbeitung eine Festlegung stattfinden wird, wer auf welche Daten in welchem Umfang zugreifen darf. Auf diese Informationen aufbauend kann ein Manager IT-Security-Prozesse installieren, um dauerhaft den Datenzugriff regelkonform zu gestalten.

Um sicherstellen zu können, dass ein Mitarbeiter immer nur die für ihn erforderlichen Zugriffsrechte zugeteilt bekommt, ist die Implementierung eines Benutzermanagements nützlich. Dieses dient im Wesentlichen der Sicherstellung korrekter Zugriffsberechtigungen vor, während und nach der Beschäftigung und der Dokumentation aller vergebenen Rechte.

5.5 IT-Security-Prozesse

5

Zu den Gründen, warum es angebracht ist, die Organisationseinheit IT-Security an die Ebene Unternehmensführung anzuhängen, gehört, dass die Führung grundsätzlich die Aufgabe hat, Entscheidungen herbeizuführen und daraus erwachsende Maßnahmen im Umfeld der IT-Security zu kontrollieren. Die Unternehmensführung delegiert in diesem Beispiel die Richtlinienhoheit und die Überwachung der Aktivitäten auf die IT-Security-Organisation. Dieser Controlling-Ansatz zieht sich durch alle Aufgabenfelder der IT-Security und erstreckt sich im laufenden Betrieb auf alle Prozesse der Datenverarbeitung. Die Kontrolle durch die IT-Security ist im Gegensatz zur Revision kein Vorgang, der im Nachhinein stattfinden sollte. Die Kontrolle sollte vielmehr in jedem Arbeitsprozess, der die Verarbeitung von Daten beinhaltet, und in jedem Projekt integraler Bestandteil sein.

5.5.1 Zugangs- und Zugriffskontrolle

Die Sicherstellung, dass Benutzer nur zu den Systemen Zugang erhalten und nur auf diejenigen Daten Zugriff bekommen, für die sie auch berechtigt sind, ist ein wesentlicher Kernpunkt der IT-Security. Neben Daten sind auch Informationen und Know-how in Form von Akten, Dokumenten und dem Wissen in den Köpfen von Mitarbeitern zu schützen. Daraus wird schnell ersichtlich, dass es um mehr geht als den Zugang per Benutzer-ID und Passwort auf Datenserver. Alle Arten von Zugängen zu Unternehmenswerten müssen geschützt werden. Neben dem Zugang über das Netzwerk ist also auch der physische Zutritt zu IT-Systemen und Akten oder die Möglichkeit, dass Mit-



arbeiter schützenswerte Informationen verraten können, so weit wie möglich abzusichern.

Hinweis

Angenommen, es würde die Speicherung von Daten auf ungeschützten lokalen Arbeitsplatzrechnern erfolgen. In diesem Fall sind die Identifikation beim Werkschutz und die Authentisierung per Mitarbeiterausweis erforderlich, um (**nach dem Zutritt zu den entsprechenden Räumlichkeiten**) Zugang zu den entsprechenden Rechnern und gleichzeitig zu den Daten zu erhalten. Aus diesem Szenario stammt die Forderung nach einer Verschlüsselung von Dateisystemen, insbesondere auf Laptops.

5

Die Schwierigkeit liegt darin, dass der Zugang zu Informationen im Allgemeinen und Daten im Speziellen auf vielfältigem Weg möglich ist. Er beginnt beim physischen Zutritt, der es einer Person ermöglichen könnte, ein entsprechendes Speichermedium aus einem Büro zu entfernen, mitzunehmen und an anderer Stelle auszulesen, es kann ihr gelingen, über das Netzwerk Zugang zu Servern zu erlangen oder aber über das Abfangen von E-Mails im Internet. Somit müssen alle möglichen Wege identifiziert und gleich hohe Schutzlevel für alle diese Möglichkeiten implementiert werden. In der IT-Security nennt man diese verschiedenen Arten, Angriffe durchzuführen, auch »Angriffsvektoren«. Bezogen auf das Beispiel aus dem Hinweis würde eine lokale Verschlüsselung der Arbeitsplatzrechner die Sicherheit erhöhen. Ein anderer Weg wäre die Abschottung der Rechner in speziell gesicherten Bereichen oder aber das Verbot, Daten lokal abzulegen. Alle diese Maßnahmen würden dazu führen, dass die Hürden für den Zugriff per Netzwerkverbindung und durch physischen Zugriff steigen.

Es ist wichtig, sich jeweils auf die Maßnahme zu konzentrieren, die letztendlich als Gewinner aus dem Vergleich von Wirksamkeit und Kosten hervorgeht, natürlich unter Beachtung der Rahmenbedingungen. Das hört sich selbstverständlich an, wird aber in vielen Fällen regelmäßig missachtet. Wenn man beim obigen Beispiel bleibt, dann wird deutlich, dass die technische Umsetzung, den Diebstahl lokal gesicherter sensibler Daten durch die Verpflichtung, diese auf Servern im Rechenzentrum zu speichern, zu verhindern, ein günstiger Weg sein kann. Müssen die Daten zu Kunden transpor-



tiert werden, dann kommt eine Verschlüsselung ins Spiel. In beiden Fällen wäre die Abschottung der Arbeitsplatzrechner in abgesicherten Büroräumen nur eine flankierende Maßnahme, würde aber nicht allen Einsatzszenarien gerecht. Letztendlich spielt auch hier die Anforderung des Kunden eine maßgebliche Rolle, in welcher Form Schutzmaßnahmen ausgestaltet werden.

Authentisierung und Autorisierung

Bevor der Zugriff auf Informationen stattfinden kann, muss sich der Benutzer, die Applikation oder das IT-System zunächst zu erkennen geben und eine erfolgreiche Authentisierung durchführen. Ist der Versuch erfolgreich, so werden die in Zugriffslisten (*access control lists*) verzeichneten Rechte freigeschaltet. Diesen Vorgang nennt man dann »Autorisierung«.

5

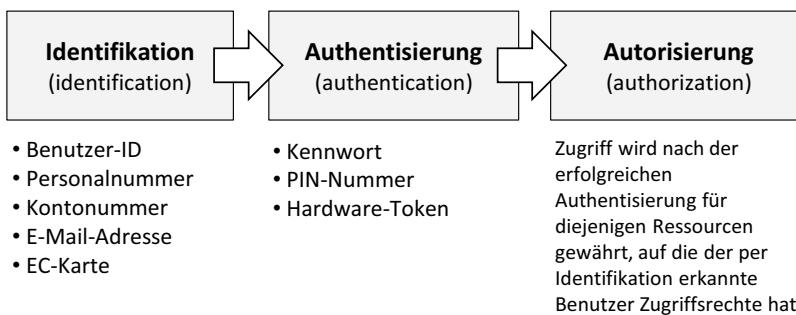


Abbildung 5.2: Zusammenhang Identifikation, Authentisierung und Autorisierung

Stellt man fest, dass die Sicherheit bei der Anmeldung per Passwort zu schwach ist, so muss der Schritt Authentisierung gestärkt werden. Der übliche Weg führt über die Zwei-Faktor-Authentifizierung. Dabei werden mindestens zwei voneinander unabhängige Methoden zur Authentifizierung genutzt, um die Hürden eines Missbrauchs durch Dritte zu erhöhen. Nachfolgend werden die drei möglichen Methoden aufgeführt:

- Über etwas, das man weiß (*what you know*). Zu dieser Gruppe gehören Kennwörter oder die Antwort auf eine geheime Frage.
- Über etwas, das man besitzt (*what you have*). Hier sind vor allem Hardware-Token und Smartcard gemeint. Auch der Schlüssel zum Rechenzentrum gehört in diese Kategorie.



- Über etwas, das zu einem gehört (*what you are*). Biometrische Eigenschaften des Benutzers wie der Augenhintergrund (Netzhaut) oder der Fingerabdruck gehören hier dazu.

Diese Methoden werden an sich bereits unterschiedlich in ihrer Stärke beurteilt. So wird einem Netzhautscan eine höhere Sicherheit zugebilligt als einem einfachen Passwort. Aufgrund der bereits gelungenen Experimente zur Umgebung dieses Verfahrens sind erhebliche Zweifel angebracht, ob diese Einschätzung auch zukünftig Bestand haben wird. Diese Einschätzung gilt für fast alle biometrischen Verfahren, die heute auf dem Markt sind. Aber auch Kennwörter haben aufgrund ihrer Beschaffenheit und ihrer Nutzung als Werkzeug zur Authentifizierung höchst unterschiedlichen Wert. Lange Kennwörter sind sicherer als kurze, sofern sie keinem Wort aus einem Wörterbuch entsprechen. Ins Kennwort eingefügte Sonderzeichen und Zahlen können die Sicherheit weiter erhöhen. Allerdings besteht wiederum die Gefahr, dass der Benutzer das Kennwort aufschreibt, was im Gegenzug dazu führen kann, dass die Sicherheit vollständig kompromittiert ist.

Tipp

Nicht selten sind Systeme, die nach wenigen, falsch eingegebenen Kennwörtern die Anmeldeprozedur für ein paar Minuten sperren, selbst bei kurzen Kennwörtern sicherer als Systeme ohne Sperre, die lange und komplexe Passwörter voraussetzen.

Aus diesen Beispielen wird schnell ersichtlich, dass es keine allgemeingültigen Regeln gibt, wann die Authentisierung sicher ist und wann nicht.

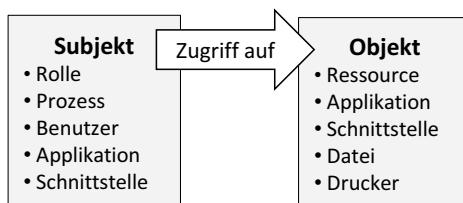


Abbildung 5.3: Beziehung Subjekt und Objekt

Neben der Authentisierung mithilfe der technischen Umsetzung einer Methode ist es möglich, mehrere Methoden zu koppeln. Mit jedem weiteren zu-



sätzlichen Mechanismus kann sich die Sicherheit enorm erhöhen. Wird nur ein Passwort genutzt, so spricht man im Übrigen von einer Ein-Faktor-Authentifizierung (*one-factor authentication*). Neben der bereits genannten, sichereren Variante der Zwei-Faktor-Authentifizierung (*two-factor authentication*) ist theoretisch auch eine Verknüpfung mit einem weiteren Faktor oder aber auch einer weiteren Person, die Passwörter einbringt, denkbar.

Zugriffskontrolle

Ein Zugriffskontrollmodell beschreibt auf einer übergeordneten Ebene, auf welche Art und Weise Benutzer Zugriff auf Ressourcen erhalten. Im einfachsten Fall werden zwischen einer Liste mit Benutzern und einer Liste mit Ressourcen Verknüpfungen hergestellt. Aus diesen kann abgelesen werden, welcher Benutzer auf welche Ressourcen Zugriff erhält. Das Zugriffskontrollmodell beschreibt also die Beziehung zwischen Benutzer und Ressource.

5

Im Wesentlichen sind drei Modelle verbreitet:

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)
- Role-Based Access Control (RBAC)

Das älteste Modell ist das **DAC-Modell**, das es seit den 1980er Jahren gibt. Auf Deutsch nennt man es im Allgemeinen besitzerbestimmte oder benutzerbestimmte Zugriffskontrolle. Dies sagt aus, dass die vollständige Kontrolle über ein Objekt beim Besitzer (*owner*) liegt. Abgeleitet davon speichern heute noch die meisten Betriebssysteme im Zusammenhang mit Daten oder anderen Ressourcen Informationen über den Ersteller und Besitzer. Der Besitzer ist jederzeit in der Lage, weiteren Benutzern Zugriff auf seine Ressourcen zu vergeben. Damit handelt es sich um ein dezentralisiertes System, innerhalb dessen jeder Besitzer einer Ressource eigenverantwortlich handelt. Benutzer, denen auf diese Art eine Berechtigung eingerichtet wurde, können ihrerseits wiederum weitere Benutzer berechtigen und ihnen sogar Rechte entziehen. Einige Unterarten von DAC setzen an dieser Stelle an und schränken die Berechtigungsvergabe ab der zweiten Ebene wieder ein. Im Zuge der Zentralisierung der Vergabe von Zugriffsrechten wurde das Recht zur Berechtigungsvergabe wieder eingeschränkt, währenddessen die ursprünglichen Zugriffsrechte erhalten blieben.



Die Einschränkungen, die MAC mit sich bringt, bergen einige Risiken, derer sich das IT-Security-Management annehmen muss. Ein Beispiel ist die Verbreitung von Schadsoftware. Da der Besitzer vollen Zugriff auf seine Objekte hat und auf alle Objekte, für die ihm explizit Rechte gegeben wurden, kann Schadsoftware, die in seinem Kontext ausgeführt wird, großen Schaden anrichten. Ein weiteres Problem ist vor allem im militärischen Bereich, dass Informationen aus einem Objekt in ein zweites kopiert werden können, und da dieses zweite Objekt vom Benutzer erstellt wurde, erhält er automatisch alle Zugriffsrechte darauf. In beiden Fällen fehlt eine weitere Sicherheitsebene, die nicht vom Benutzer, sondern vom Objekt abhängig ist. Dieses Manko beseitigt das MAC-Modell weitgehend.

Das **MAC-Modell** berücksichtigt neben dem Benutzer und dem Ressourcenobjekt weitere Kriterien, um Zugriffsrechte zu erteilen oder zu verweigern. Dieses Prinzip ist vor allem im militärischen bzw. Hochsicherheitsbereich wichtig. In diesen Fällen werden Ressourcenobjekten weitere Einstufungen zugeordnet, die eine Klassifizierungsrichtlinie oder auch andere Kataloge zur Grundlage haben können. Im militärischen Bereich würde man einem Objekt zusätzlich eine Sicherheitsklasse zuordnen. Diese bezieht sich auf das Objekt in jedem Stadium seiner Existenz und beinhaltet automatisch auch alle weiteren Objekte, die von diesem Objekt erben. Auf der anderen Seite wird jedem Benutzer eine Sicherheitseinstufung zugeordnet. Die Regeln, die nun entscheiden, ob der Zugriff autorisiert wird, basieren auf der Frage, ob die Sicherheitseinstufung des Benutzers mit der Sicherheitsklasse des gewünschten Objekts korrespondiert.

Eine bekannte Ausprägung des MAC-Modells ist das Bell-LaPaluda-Modell. Es soll sicherstellen, dass Objekte einer höheren Sicherheitsklasse nicht gelesen werden können und dass es zudem nicht möglich ist, die Sicherheitsklasse eines solchen Objekts nach unten zu verändern. Damit zielt das Bell-LaPaluda-Modell auf die Vertraulichkeit von Daten. Sicherheitsklassen für Objekte können z.B. folgendermaßen gestaffelt sein:

- Top Secret/Streng geheim
- Secret/Geheim
- Confidential/Vertraulich
- Unclassified/Öffentlich



Da die Sicherheitsklasse an das jeweilige Objekt gebunden ist, findet die Entscheidung, ob ein Zugriff erlaubt wird oder nicht, üblicherweise auf dem IT-System statt, auf dem die jeweiligen Objekte abgelegt sind.

Auf die Integrität von Daten zielt das zweite, exemplarisch genannte Modell, das Biba-Modell. In dieser Spielart basiert der Zugriff auf Integritätsstufen anstelle von Zugriffsstufen, die vor allem aus Sicht des Lesezugriffs erstellt wurden. In diesem Modell wird ein Subjekt, ein Benutzer oder ein IT-System mit niedriger Integritätsstufe ein Objekt mit höherer Integritätsstufe nicht verändern dürfen.

Das dritte Modell, das **RBAC-Modell**, basiert auf Rollen, die den Zugriff auf Ressourcen regeln. Rollen werden verwendet, um die Arbeitswirklichkeit möglichst nahe abzubilden. Aus diesem Grund sind Rollen wie »Wareneingang« oder »PC-Hotline« üblich. In beiden Fällen repräsentieren die Rollen eine Reihe von definierten Berechtigungen auf Ressourcen. Benutzer werden jeweils einer Rolle zugewiesen, anstatt sie direkt für Objekte zu berechtigen. Das hat viele Vorteile wie Transparenz und Übersichtlichkeit und ermöglicht Anpassungen der Rollen, ohne jede Verknüpfung von Benutzer und Objekt anfassen zu müssen.

5

Wichtig

Ein Benutzer kann grundsätzlich mehrere Rollen innehaben. Dabei ist zu beachten, dass Rollen nach dem Prinzip der Funktionstrennung (*segregation of duties*) zugeordnet werden. Dabei darf ein Benutzer nicht die Rollen »Wareneingang« und »Wareneingang Verbuchung« gleichzeitig innehaben, da dies den Missbrauch ermöglichen würde.

Das RBAC-Modell wird heute mit Abstand am häufigsten in der Industrie eingesetzt. Solange keine Anforderungen ähnlich wie im Militärbereich erforderlich sind, verbindet es die Vorteile von MAC mit der Administrierbarkeit von Gruppenberechtigungen. Produkte wie das Active Directory von Microsoft, der Microsoft SQL Server, Windows-Betriebssysteme und Linux nutzen dieses Modell.



5.5.2 Sicherheit von Software

Die Installation, Konfiguration und Wartung von IT-Systemen gehört zum täglichen Handwerk der IT-Abteilung. In fast allen Fällen ist auch komplexe Software mit im Spiel. Selbst Messstationen wie z.B. Temperaturfühler können heute mehr als nur Daten erfassen. Sie können bei der Über- oder Unterschreitung von Schwellenwerten alarmieren und ihre Daten über das Netzwerk an Server schicken, auf denen diese Daten ausgewertet werden. Wenn es um Software geht, dann sind die Aufgaben der Konfiguration und des Patchmanagements immer präsent. Und auf die IT-Security bezogen: Immer, wenn Software vorhanden ist, muss diese gegen Angriffe und gegen missbräuchliche Benutzung abgesichert werden.

Wichtig

Die EU-DSGVO spricht im Zusammenhang mit der Verarbeitung von personenbezogenen Daten von Rechten der Betroffenen und Pflichten der verarbeitenden Stelle. Beides ist im Zusammenhang mit der Nutzung von Software von großer Bedeutung. Explizit wird bei der Datenverarbeitung von »Privacy by Design« und »Privacy by Default« gesprochen. In einem Projekt, das den Zweck hat, Software einzuführen, müssen beide Prinzipien von Beginn an beachtet werden. Der Datenschutz ist damit eine der wichtigsten Leitplanken, wenn es darum geht, zu ermitteln, was aus Gründen der Compliance umgesetzt werden muss und wie dies zu erfolgen hat. Das »Recht auf Vergessen« und das Recht auf »Auskunft über die Datenverarbeitung der eigenen personenbezogenen Daten« stellen Softwarehersteller zudem vor große Schwierigkeiten. Daten aus einer Datenbank zu löschen, ist grundsätzlich nicht schwierig, sofern man das Design so wählt, dass Inkonsistenzen aufgrund dieses Vorganges technisch unterbunden werden. Innerhalb des Daten-Lifecycles existiert eine solche Datenbank häufig aber auch in einem Backup oder einem Offline-Archiv. In diesen Fällen ist das Löschen schon sehr viel schwieriger zu handhaben.

5

Grundsätzlich gilt, dass es sich lohnt, zu Beginn eines Softwareprojekts darauf zu achten, dass der Lieferant eine technische Lösung für diese Heraus-



forderungen bereitstellt, dass der Datenschutzbeauftragte von vornherein involviert ist und die Lösung abgenommen hat und dass personenbezogene Daten von den restlichen Daten so getrennt gespeichert werden, dass die einen gelöscht oder pseudonymisiert werden können, ohne die anderen nutzlos zu machen. Naturgemäß liegt der Schwerpunkt der Überlegungen hinsichtlich der Implementierung und Konfiguration von Software nicht im Bereich der IT-Security, sondern vor allem darin, Anforderungen von Kunden zu entsprechen. Der Verantwortliche für IT-Security hat demnach zunächst die Aufgabe, Grundsätze über die Planung, die Inbetriebnahme und die Wartung von IT-Systemen zu definieren. Damit bildet er ein Gerüst, innerhalb dessen sich die Umsetzung der Anforderungen der Kunden bewegen muss. Nur wenn dieses Gerüst im Vorfeld bekannt ist, dann wird eine sinnvolle Planung möglich sein. Die Kontrolle, ob alle Vorgaben eingehalten werden, bildet dann den Kern der sicherheitstechnischen Aufgabe.

Softwarequalität

Software lässt sich in verschiedene Kategorien unterteilen. Jede Kategorie folgt eigenen Gesetzen, was die Betrachtung vonseiten der IT-Security angeht, und deshalb ist eine jeweils darauf angepasste Vorgehensweise zu empfehlen.

Kategorien an Software:

- Eigenentwickelte Software, siehe folgendes Kapitel
- Im Auftrag entwickelte Software
- Kaufsoftware
- Software, die im Rahmen eines Application Service Providers (ASP) z.B. über das Internet genutzt wird. Die Nutzung findet über dedizierte Server eines Anbieters oder im Rahmen der Nutzung einer Cloud-Dienstleistung statt.

Wird Software selbst entwickelt oder im eigenen Auftrag durch Dritte realisiert, so folgt der Prozess der Entwicklung den Vorgaben aus den entsprechenden Pflichten- und Lastenheften. Sicherheitsaspekte werden in jeder Phase betrachtet werden müssen. Dies reicht von den ersten Überlegungen im Rahmen des Softwaredesigns bis hin zum Rollout und zur Wartung. Für die Softwareentwicklung ist eine Reihe von Qualitätsmerkmalen weithin anerkannt. Neben der Abdeckung der vom Auftraggeber geforderten Funktionalität sind dies die Sicherheitsziele Vertraulichkeit, Verfügbarkeit, Belast-



barkeit aus der EU-DSGVO und Integrität. Aus Sicht eines Softwareprodukts bedeutet dies, dass Software keine Schwachstellen aufweisen darf, die einem Angreifer nicht-autorisierten Zugang erlauben würden. Um die Verfügbarkeit gewährleisten zu können, muss Software stabil und möglichst wenig anfällig für fehlerhafte oder unerwartete Bedienung sein. Die Belastbarkeit zielt auf einen ganzheitlichen Ansatz, der neben der Verfügbarkeit der Software auch alle weiteren Komponenten beinhaltet, die Einfluss darauf nehmen können, dass die Daten unter Umständen nicht mehr zur Verfügung stehen. Wenn man das weiter denkt, dann wird schnell klar, dass es, wenn es um die Verarbeitung personenbezogener Daten geht, nicht damit getan ist, eine Software von DVD zu installieren, als Betreiber muss man sich deutlich weiter gehende Gedanken machen und auch deutlich mehr Stellen in der IT und auch außerhalb mit einbeziehen. Wie dieses neue Schutzziel letztendlich in der Realität gelebt werden wird, ist allerdings noch weitgehend offen. Mechanismen zur Kontrolle von Eingaben und eine implementierte Datensicherung stellt zudem die Integrität der verarbeiteten Daten sicher.

Viele dieser Punkte werden in den Vorgaben der DIN 9001 behandelt. Ein entsprechendes Qualitätshandbuch legt die Anforderungen fest und definiert die Rahmenbedingungen, in denen sich die Softwareentwicklung bewegt.

Der Einfluss auf die Qualität von Kaufsoftware hängt stark von der Marktstellung des Anbieters und seiner Flexibilität ab. Sehr häufig werden Verbesserungen über Änderungen an der Konfiguration und über angebotene Patches wahrgenommen. Der Vergleich zwischen den Sicherheitsmechanismen der angebotenen Software und den eigenen Anforderungen zeigt dann auf, ob die jeweilige Software aus Sicht der IT-Security infrage kommt. Eine angebotene Software auf ihre Sicherheit zu testen, ist aufwendig und kostspielig. Sehr häufig geschieht dies in Form einer Testinstallation und einem nachfolgenden Penetrationstest. Dabei untersuchen zumeist externe Spezialisten die Software auf Lücken und Fehler. Der Vergleich und die Bewertung gefundener Sicherheitslücken mit den eigenen Sicherheitsanforderungen ist dann der zweite Schritt. In dem dabei zugrunde gelegten Anforderungskatalog müssen Sicherheitsziele deshalb eine prominente Stelle einnehmen.

Die Nutzung von Software als Onlinedienstleistung, z.B. über das Internet, macht die Überprüfung und Einschätzung des Umsetzungsgrades von Sicherheitsanforderungen schwierig. Um in diesen Fällen auf bestehende Risiken zu reagieren, bleibt oftmals nur die Verlagerung des Risikos auf Dritte, sprich



eine vertragliche Regelung, die Risiken zum Dienstanbieter verschiebt. Aber auch in diesem Fall ist einem Unternehmen selten geholfen, wenn sensible Daten auf Servern abgelegt sind, deren Standort nicht bekannt ist. Speziell in diesen Fällen wird das Thema Datenschutz von einiger Wichtigkeit sein.

Planungsphase

Jedes IT-System und jede Applikation durchläuft mehrere sicherheitsrelevante Stadien. Zunächst findet die Planungsphase statt, in der es wichtig ist, mögliche Schwachstellen im Vorhinein zu identifizieren und in der weiteren Planung zu berücksichtigen. Fehler, die in dieser Phase gemacht werden, wirken sich auf alle weiteren Schritte bis hin zum Betrieb aus und sind im Nachhinein nur unter erhöhtem Aufwand wieder zu bereinigen. Zu den hierbei zu betrachtenden Punkten gehören:

5

- Die Reputation des Herstellers und eine Abschätzung, ob sich dieser noch über den benötigten Zeitraum im Markt behaupten kann. Zusätzliche Fragen sind, ob laufend Sicherheitspatches bereitgestellt und die Applikation oder das IT-System laufend weiterentwickelt wird.
- Die Möglichkeit, während des Projekts und in der Betriebsphase auf Expertenwissen zugreifen zu können. Das betrifft sowohl interne als auch externe Ressourcen.
- Wie werden Daten innerhalb des Systems verarbeitet und entspricht dies den formalen Anforderungen? Zu betrachten ist der gesamte Weg, den Daten nehmen. Wird eine Applikation auf einem Server installiert, so beginnt dieser Weg spätestens beim Benutzer, der Daten darin einpflegt, reicht über die Ablage in einem Dateisystem oder in einer Datenbank bis hin zur Datensicherung und einer Archivierungslösung.
- Entspricht die angedachte Lösung der Klassifizierung der Daten, die damit verarbeitet werden sollen? Viele Lösungen mögen pragmatisch und funktional sein, entsprechen aber nicht der Sicherheitseinstufung, die z.B. für geheime Daten nötig wäre.

Implementierungsphase

Die Installation von Betriebssystemen, die Aufstellung und das Anschließen von Hardware an ein Netzwerk und das Ausrollen von Software bezeichnen die Projektphasen, in der die erarbeiteten Vorgaben im Rollout umgesetzt



werden. In dieser Phase ist es wichtig, dass die Umsetzung so erfolgt, dass sie mit den definierten Sicherheitskriterien zusammenpasst und dass alle Vorgänge dokumentiert werden. Die Dokumentation liefert später den Nachweis, wie installiert wurde, und Anhaltspunkte im Fehlerfall. Für den Verantwortlichen für IT-Security stellt sie die Grundlage für ein erstes Audit dar.

Während der Implementierung findet im Allgemeinen auch die erste Konfiguration statt. Mit dem Ziel vor Augen, möglichst rasch zum gewünschten Ergebnis zu gelangen, schleichen sich hier häufig Ungenauigkeiten ein. Wird z.B. festgestellt, dass der Zugriff auf die Datenbank über die Firewall nicht funktioniert, da weitere Ports freigeschaltet werden müssen, so liegt es nahe, im herrschenden Zeitdruck zunächst einmal alle Regeln zu deaktivieren, um die Installation zu einem Ende zu bringen. Dies ist nur ein Beispiel für typische Vorgänge während einer Implementierung. Solange keine hoch klassifizierten Daten durch das frisch aufgesetzte System verarbeitet werden, ist dies nicht weiter kritisch. Anders sieht es aus, wenn diese kurzfristigen Ausnahmen bis zum Beginn des Echtbetriebs nicht wieder korrigiert werden.

Betrieb

Geht ein neues System oder eine neue Applikation von der Projektphase in den Betrieb über, dann findet zunächst eine Übergabe statt, da der Personenkreis im Projekt häufig ein anderer ist als der, der das System nachher betreibt. Die Installationsdokumentation, ein Betriebshandbuch und eventuell noch eine Liste offener Sicherheitsprobleme stellen die Arbeitsgrundlage für den Betreiber dar.

Neben den im Betriebshandbuch beschriebenen Prozessen und Anweisungen, wie auf Probleme zu reagieren ist, sind Wartungsverträge eine weitere Voraussetzung für die Sicherstellung der Verfügbarkeit. Der Umfang und damit die Kosten für einen Wartungsvertrag lassen sich von den definierten Service Level Agreements (SLA) und den Ergebnissen einer Business-Impact-Analyse ableiten. Der zweite Punkt kommt aus der Business-Continuity-Planung und beschreibt allgemein die Schäden für das Unternehmen, die bei einer Nichtverfügbarkeit entstehen würden.

Zur Instandhaltung gehört grundsätzlich auch die Sicherstellung, dass die jeweils zugrunde liegenden IT-Systeme immer technisch auf dem neuesten Stand sind. Um dies sicherzustellen, sind sowohl regelmäßig Sicherheits-



updates einzuspielen als auch dafür Sorge zu tragen, dass die Konfiguration den Sicherheitsbestimmungen genügt. Das reicht von der Benutzerverwaltung bis hin zu technischen Einstellungen.

Ein weiterer wichtiger Bestandteil des Betriebs ist die Anfertigung und die ständige Aktualisierung von Notfallplänen. Wiederum abhängig von der Business-Impact-Analyse dienen diese Pläne als Vorsorge für den Krisenfall und beinhalten alle Dokumente, die erforderlich sind, um auf Schäden bis hin zum Wiederanlauf des IT-Systems und der Neuinstallation und Konfiguration der darauf installierten Software zu reagieren.

5.5.3 Sichere Softwareentwicklung

5

Software zu entwickeln, wird immer leichter und intuitiver. Entwicklungsumgebungen, in denen man zu einem großen Teil mit grafischen Werkzeugen zugange ist und nur ab und zu Kontakt zum eigentlichen Quelltext hat, setzen sich allmählich durch. Eines hat sich aber bis heute nicht geändert: Je komplexer eine Software wird, desto mehr Schwachstellen wird sie enthalten und desto mehr Bedrohungen können zu einem Risiko werden. Es ist demnach heute noch mindestens genauso wichtig, jede Phase der Softwareentwicklung auch unter dem Gesichtspunkt der IT-Security zu betrachten, wie es in der Vergangenheit der Fall war.

Hinweis

Falls der Manager IT-Security nicht auch Softwareentwickler ist und damit aufgrund seines Wissens tief in die Materie eintauchen kann, dann hat er zumindest die Pflicht, auf sichere Prozesse innerhalb des Softwareentwicklungsprozesses hinzuwirken, diese zu überwachen und entsprechende Regelungen zu erstellen.

Konzepte, Software sicher zu erstellen, gibt es einige. Projekte wie »Security by Design«, ein Begriff, den Microsoft aktuell prägt, oder das »Open Web Application Security Project« (OWASP) zeigen Wege und Mittel auf, sich dieser Aufgabe zu nähern. Zumindest die Grundzüge dieser Ansätze sollte der Manager IT-Security kennen, um als Sparringspartner der Softwareentwickler



fungieren zu können. Tief gehende Programmierkenntnisse sind dabei nicht erforderlich.

Als Manager IT-Security kann man den Prozess der Softwareentwicklung hinterfragen und die grundlegenden erforderlichen Rahmenbedingungen abfragen. Die wichtigsten Themen greift die nachfolgende Tabelle auf.

Themenbereich	Erläuterungen
Verantwortlichkeiten, Rollen	Jedes Softwareprojekt muss so strukturiert sein, dass Rollen wie »Zuständig für Softwaresicherheit« oder »Zuständig für Testmaßnahmen« klar vergeben sind. Der Manager IT-Security muss einen direkten Ansprechpartner haben, dem er seine Fragen stellen und seine Anforderungen übergeben kann. Dieser Ansprechpartner ist letztendlich verantwortlich für die korrekte Umsetzung von Vorgaben. Zumindest in Projekten, die in erhöhtem Maß sicherheitsrelevant sind, sollte der Manager IT-Security ein Review der Softwarearchitektur vornehmen und in den Freigabe-Prozess aktiv eingebunden sein.
Fachwissen im Bereich Softwaresicherheit	Der Verantwortliche für die Softwaresicherheit innerhalb des Projekts und Ansprechpartner des Managers IT-Security muss über das erforderliche Fachwissen verfügen. Dazu muss er jede Station des Software-Lifecycles und die jeweiligen Risiken für die Softwaresicherheit kennen und entsprechende Maßnahmen zuordnen können.
Qualitätsmanagement	Softwaresicherheit ist ein weiteres Qualitätsmerkmal in der Softwareentwicklung. Andere Merkmale sind Stabilität, Performance, Belastbarkeit gegen Angriffe oder Skalierbarkeit. Alle diese Merkmale werden im Rahmen des Qualitätssicherungsprozesses untersucht und im Falle von Defiziten mit korrigierenden Maßnahmen unterlegt. Das Pflichtenheft muss die Anforderungen an die Qualität der Softwaresicherheit detailliert beschreiben. Auf Basis dieser Vorgaben kann der Verantwortliche für die Qualität zusammen mit dem Verantwortlichen für Softwaresicherheit die Prüfungen vornehmen.



Themenbereich	Erläuterungen
IT-Systeme	<p>Der Arbeitsplatzrechner des Softwareentwicklers, eine gemeinsam genutzte Datenbank und das Netzwerk müssen sicher sein. Ein Angriff auf den Quelltext während der Softwareentwicklung muss ausgeschlossen werden. Das reicht von der Installation einer Antivirensoftware bis hin zur Abschottung der Entwicklungsumgebung mithilfe einer Firewall.</p> <p>Neben dem Schutz der Infrastruktur muss auch der Quelltext an sich geschützt werden. Dies kann durch Quelltextverschleierung (<i>obfuscation</i>) oder durch einfache Entfernung von Kommentaren geschehen. Wird weitere Verwaltungssoftware genutzt, z.B. zur Versionierung, dann müssen auch diese IT-Systeme geschützt werden.</p>
Implementierung	<p>Vorgaben an die Softwaresicherheit erstrecken sich auch auf die Implementierung. Ein Kriterium wie die Vergabe von Zugriffsrechten muss den Vorgaben entsprechend konsequent umgesetzt werden.</p>
Wartung und Weiterentwicklung	<p>Die Weiterentwicklung der Software muss neben sich ändernden Anforderungen der Kunden auch stets die Softwaresicherheit im Auge behalten. Neue Entwicklungen auf Seiten der potenziellen Angreifer können neue Maßnahmen zur Softwaresicherheit erforderlich machen.</p> <p>Jede Erweiterung oder Veränderung der Software muss weiterhin einem Qualitätssicherungsprozess unterworfen sein, der auch das Merkmal Softwaresicherheit beinhaltet.</p>

5.5.4 Identitätsmanagement

Das Identitätsmanagement (*identity management*) kümmert sich um die Verwaltung von Identitäten. Die Verwendung des Begriffs »Identitäten« zeigt schon, dass es nicht nur um natürliche Personen geht, die als zugreifendes Subjekt verwaltet werden müssen, sondern dass sich das Gebiet genauso auch um Identitäten wie Service-User kümmern muss, die dazu dienen, Applikationen auf Servern mit Rechten auszustatten. Hinter einem Benutzer-Account »MAIUWE1«, der letztendlich für den Zugriff auf Daten genutzt wird, steht eine physische Identität, nämlich Herr Uwe Maier. Der Benutzer-Account wird in diesem Fall als digitale Identität bezeichnet. Ist der Zusammenhang zwischen physischer und digitaler Identität nicht offen erkennbar, so kann es sich auch um eine virtuelle Identität handeln.



Der Account eines Mitarbeiters hat eine ganze Reihe an Attributen, die von verschiedenen Systemen unterschiedlich genutzt werden. So gehört die Telefonnummer des Mitarbeiters genauso verwaltet wie dessen Adresse oder Geburtsdatum. Einige dieser Daten sind dem Datenschutzgesetz unterworfen, andere nicht. Manche Informationen nutzt man zur Authentifizierung und andere wiederum für die Freischaltung von Zugriffsberechtigungen.

Im Folgenden konzentrieren wir uns auf Personen und ihren Zugang zu Daten und IT-Systemen.

Wichtig

Zu wissen, wem welche Rechte und damit Berechtigungen zugeteilt sind, ist die Grundlage dafür sicherzustellen, dass zu jedem Zeitpunkt nur die Rechte zugeteilt werden, die der Mitarbeiter zum Arbeiten benötigt.

5

Ein Großteil der Mitarbeiter arbeitet mit vielen unterschiedlichen IT-Systemen. Zusätzlich greifen auch Berater, Kunden und Lieferanten auf diese IT-Systeme zu. Zudem werden eigene Daten durch externe Firmen, z.B. in Form von Internetportalen, weiteren Personenkreisen zur Verfügung gestellt. Das Identitätsmanagement beinhaltet alle Prozesse, um Personen Rechte auf den IT-Systemen zuzuteilen, die von ihnen benötigt werden. Diese Zuteilung läuft gesteuert ab und geht über die reine Zuweisung von Rechten weit hinaus und betrifft genauso die Dokumentation, d.h. Nachvollziehbarkeit, und die Automatisierung dieser Vorgänge.

Phasen der Anstellung

Ein Mitarbeiter durchläuft drei Phasen der Beschäftigung in einem Unternehmen:

- Vor der Einstellung
- Während der Anstellung
- Beendigung des Arbeitsverhältnisses

In jeder dieser Phasen sind die kontrollierte und dokumentierte Vergabe von Zugriffsrechten und die Zurverfügungstellung von Gerätschaften zu regeln und zu kontrollieren.



KAPITEL 5 – BETRIEB DER IT-SECURITY

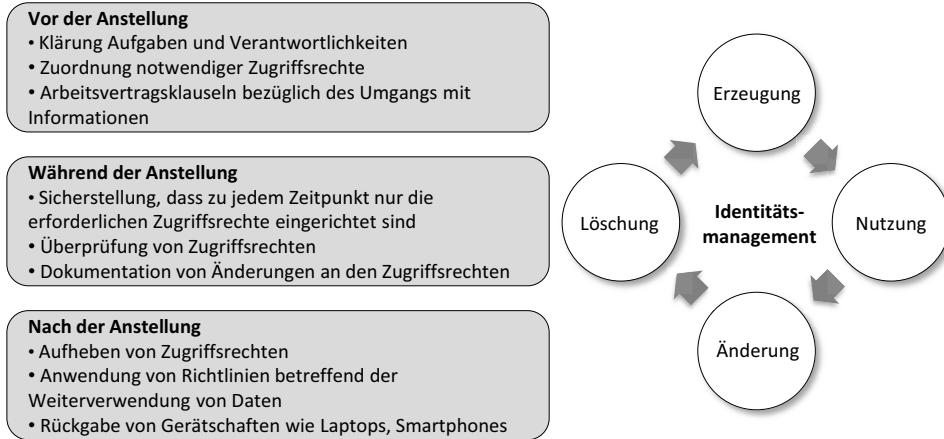


Abbildung 5.4: Phasen der Anstellung

5

Es beginnt mit der **Einstellung**, die mit einer ersten Vergabe von Zugriffsrechten und der Ausstattung mit Gerätschaften einhergeht. Die Zuordnung eines Arbeitsplatzrechners oder eines Laptops ist Bestandteil dieser ersten Phase. Schon vor der Einstellung müssen vertragliche Regelungen getroffen werden, was die Behandlung von Informationen während und nach der Beschäftigung betrifft. Im Rahmen des Arbeitsvertrags getroffene Regelungen sind an Verbindlichkeit später nicht mehr durch weitere Vereinbarungen ohne Weiteres erreichbar.

Jeder Mitarbeiter muss seine Rechte und Pflichten kennen, diese akzeptieren und danach handeln. Die missbräuchliche Nutzung von Informationen muss dementsprechend Disziplinarmaßnahmen nach sich ziehen. Voraussetzung dafür und Grundlage für das gesamte Identitätsmanagement ist, dass die Grundzüge von der Unternehmensleitung festgelegt und kommuniziert werden.

Während der Anstellung durchläuft ein typischer Angestellter eine Reihe von Funktionen mit häufig sehr unterschiedlichen Zugriffsrechten auf Daten verschiedener Bereiche. Jede Änderung der Funktion muss demnach einen Prozess starten, der die bestehenden Zugriffsrechte überprüft und gegebenenfalls neue hinzufügt und alte entfernt. Die Grundlage der dadurch erforderlichen Entscheidungen ist der Grundsatz, dass jeder Mitarbeiter nur auf diejenigen Daten und Informationen generell Zugriff erhält, die er für seine Arbeit benötigt.



Mit der **Beendigung des Arbeitsverhältnisses** schließlich müssen Betriebsmittel und vor allem auch Zugriffsrechte wieder entzogen werden. Neben der Rechtezuteilung muss unter Beachtung des Datenschutzgesetzes und anderer Vorgaben auch über die weitere Behandlung von Daten entschieden werden, die der Benutzer erzeugt hat. Dieser Punkt ist häufig mit am schwierigsten und birgt einige Sicherheitsrisiken. Ein Beispiel ist die E-Mail-Datenbank des Benutzers mit der gesamten Korrespondenz mit Kunden. Es ist nachvollziehbar, dass sein Nachfolger oder ein Kollege oder Vorgesetzter Zugriff auf diese Korrespondenz benötigt, um die Arbeit sinnvoll weiterführen zu können. Unter Umständen hat sich aber im Laufe der Jahre zusätzlich eine Menge an Informationen in dieser Datenbank angesammelt, auf die ein Kollege nicht zugreifen darf, da sie private oder auch generelle personenbezogene Informationen enthalten. Eine leichte Lösung gibt es für ein solches Dilemma nicht. Wurde nicht im Vorfeld technisch Vorsorge dafür getroffen, dass sich nur die Daten in der Datenbank befinden können, die unkritisch sind, und alle private Korrespondenz separat davon aufbewahrt wurde oder aber die Nutzung für private Zwecke generell untersagt wurde und die Umsetzung auch laufend überprüft wurde, dann muss ein Prozess und eine abgestimmte Regelung implementiert werden, der unter Einbezug des Datenschutzbeauftragten die Daten durchforstet und entsprechend die Zugriffsrechte neu zuweist.

Toolgesteuerter Prozess

»Bei Beendigung der Anstellung oder auch der Änderung des Anstellungsverhältnisses ist es erforderlich, die getätigten Zugriffsrechte wieder aufzuheben.« Das hört sich einfacher an, als es in vielen Unternehmen tatsächlich ist. Es kommt nicht nur in großen Unternehmen vor, dass es zu einem Benutzer eine ganze Reihe von zugeordneten Benutzer-IDs in den verschiedensten IT-Systemen gibt. Alle Bereiche, die unter Umständen eine solche ID ausgestellt haben, müssen rechtzeitig informiert werden, um dann auch tätig werden zu können. Das Gleiche gilt für den Fall, dass ein Mitarbeiter von Bereich A nach Bereich B wechselt.

Zwischen 40 % und 60 % der typischen Arbeit eines Helpdesks besteht in der Anlage von Benutzern und der Vergabe und dem Entzug von Zugriffsrechten. Die Benutzerverwaltung ist die operative Aufgabe, die neben dem Problemmanagement die meiste Zeit in der Abarbeitung von Arbeitsaufträgen in



KAPITEL 5 – BETRIEB DER IT-SECURITY

Anspruch nimmt. Geschieht diese Arbeit ohne weitere Unterstützung durch Tools, so stehen die Mitarbeiter immer wieder vor Entscheidungen, die sie im Grunde nicht verantworten können. Soll diese Person Zugriff auf dieses Verzeichnis erhalten? Im Grunde ist in diesem Fall die Zustimmung des Besitzers des Verzeichnisses zu erfragen. Bei Hunderten Änderungen pro Woche wird dies aber nicht lückenlos geschehen, und schon entstehen Lücken in der Berechtigungsstruktur und damit auch im Sicherheitsniveau. Um diesen Zustand zu ändern, sind verschiedene Tools auf dem Markt.

Die Anforderungen an den Einsatz eines Tools zum Identitätsmanagement sind unter anderen die folgenden:

- Dokumentation, wer wann wem welche Zugriffsrechte zugeordnet hat
- Ausschließen des direkten Zugriffs durch einen Administrator. Das Umgehen der durch das Tool definierten Prozesse ist kontraproduktiv und sollte verhindert werden.
- Ermöglichen eines Änderungsmanagements bei Wechsel von Mitarbeitern zwischen Bereichen oder im Falle des Ausscheidens aus dem Unternehmen
- Entlastung des Benutzersupports und der Hotline
- Ermöglichung von Massenänderungen wie z.B. bei der Umbenennung von Organisationsstrukturen
- Automatisieren von Benutzeranlagen
- Alle Vorgänge müssen standardisiert sein.
- Möglichst viele IT-Systeme sollten in das Tool integriert werden können.

Ein gutes Tool dokumentiert alle benutzerbezogenen Vorgänge lückenlos. Dies beginnt bei der Anlage einer oder mehrerer Benutzer-IDs, der Erstellung entsprechender persönlicher Datenverzeichnisse und die Berechtigungsvergabe, die an die Rolle des Mitarbeiters gekoppelt ist. Änderungen an den Rechten werden durch automatisierte Workflows abgearbeitet. Diese beginnen mit einem Antrag auf Zugriffsrechte, gehen über die Freigabe des Besitzers der Daten, häufig der Vorgesetzte, und enden in der automatisierten Vergabe der Rechte und der Dokumentation, wer sie beantragt und wer sie freigegeben hat.



5.5.5 Genehmigungsprozesse

Die IT-Security-Organisation hat neben einer beratenden Tätigkeit auch die Aufgabe, Entscheidungen bezüglich Strategien, Regeln und der Abarbeitung von Einzelfällen zu treffen. Aufgrund der Expertise und der größeren Übersicht macht es Sinn, die Verantwortlichen für IT-Security in Entscheidungsworkflows mit einzubinden.

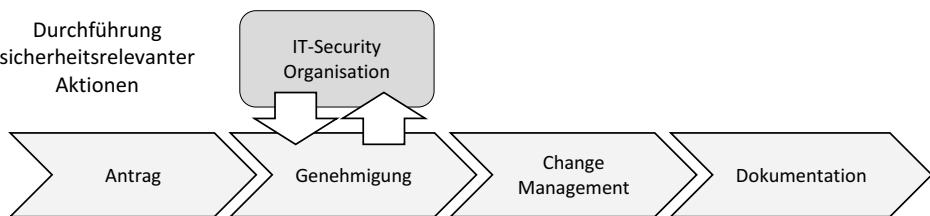


Abbildung 5.5: Genehmigungsprozess unter Einwirkung der IT-Security-Organisation

In Abbildung 5.5 ist ein exemplarischer Prozess dargestellt, in dem alle Stationen vom Benutzer bis hin zur Durchführung seines Antrags erscheinen. Der Benutzer will in diesem Fall eine Funktionalität nutzen, die nicht ad hoc an seinem Arbeitsplatzrechner funktioniert: Er möchte eine Datei per FTP-Protokoll auf einen Server im Internet kopieren. Im Normalfall wird er sich mit seinem Anliegen an die Hotline wenden, die wiederum ein Ticket erstellt und dieses an den Experten in der IT weiterleitet. Dieser Experte erkennt, dass die Umsetzung eine neue Regel an der Firewall benötigt und dass dazu die Freigabe der IT-Security-Organisation erforderlich ist. Also sendet er den Antrag weiter an den entsprechenden Verantwortlichen. Dieser muss nun eine Entscheidung treffen. Idealerweise basiert diese auf einer bestehenden Regelung, die z.B. besagt, dass dieser Vorgang grundsätzlich verboten ist, da FTP unverschlüsselt überträgt, oder aber, dass eine individuelle Risikoprüfung erforderlich ist. Wir nehmen an, der zweite Fall trifft zu. Das bedeutet, dass im Gespräch mit dem Antragsteller zunächst geprüft werden muss, wie die Daten einzustufen sind. Handelt es sich um unkritische Daten, dann kann der Zugriff eventuell schon gestattet werden. Handelt es sich um sensible Daten, dann kann der Vorgang entweder komplett verboten und dem Benutzer Alternativen aufgezeigt werden oder aber zusätzliche Maßnahmen genannt werden, mit deren Unterstützung das Risiko auf ein vertretbares



Maß reduziert werden kann. In unserem Fall könnte man sich vorstellen, dass die Daten vor der Übertragung verschlüsselt werden, das Passwort per Telefon mit dem Betreiber des Zielrechners ausgetauscht wird und dass in dieser Konstellation auch die Einrichtung einer Regel gestattet werden kann.

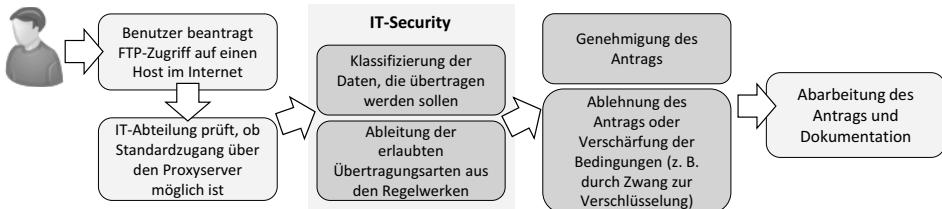


Abbildung 5.6: Genehmigungsprozess

5

Der beschriebene Vorgang sagt aus, dass eine Regel an der Firewall eingerichtet wird, die einem bestimmten Vorgang geschuldet ist. Nach Wochen oder Monaten wird sich vermutlich niemand mehr daran erinnern, warum es diese Ausnahme gibt und wozu sie dient. Aus diesem Grund ist es wichtig, alle Stationen des Workflows zu dokumentieren. In Abbildung 5.6 ist dies beispielhaft dargestellt. Die Dokumentation beinhaltet Informationen darüber, wer den Antrag gestellt hat, welche Kriterien zur Entscheidung über die weitere Vorgehensweise geführt haben und wie schlussendlich verfahren wurde.

5.5.6 Standardisierung

Um das Ziel eines einheitlichen Sicherheitsniveaus erreichen zu können, muss ein großer Teil der IT-Landschaft standardisiert werden. Grundsätzlich gilt, je weniger Ausnahmen es bei Soft- und Hardware sowie den Arbeitsprozessen gibt, desto weniger hoch ist der Aufwand, durch technische und organisatorische Maßnahmen Sicherheit zu erreichen. Neben den offenkundigen Einsparungen, die im Zuge der Vereinheitlichung von Prozessen erzielt werden können, stellen sie auch einen der wichtigsten Wege dar, die Anforderungen aus der EU-DSGVO zu erfüllen. In diesem Fall geht der Nutzen weit über den IT-Bereich hinaus. Definierte Prozesse, was die Benutzerverwaltung, die Installation neuer Software, Genehmigungsprozesse von Public-Cloud-Lösungen oder den automatischen Einbezug des Datenschutzbeauftragten angeht, dienen dazu, die durch die IT unterstützten Betriebsprozesse in die gesetzlich geforderte Richtung zu bewegen. Die EU-DSGVO fordert, dass ein Unternehmen zu jedem Zeitpunkt weiß, wo sich die personenbezogenen Daten eines



jeden Mitarbeiters befinden. Eine solche Vorgabe ohne strukturierte und vereinheitlichte Datenspeicherungskonzepte zu lösen, ist sehr schwierig und aufwendig.

Die Werkzeuge der Datenverarbeitung, also vor allem Arbeitsrechner, Server, Netzwerkkomponenten und die darauf installierte Software, können heute vorkonfiguriert und vereinheitlicht zur Verfügung gestellt werden. Entscheidend ist dabei die Anzahl unterschiedlicher Produkte. Wenn für jede Aufgabenstellung nur einige wenige Produkte im Einsatz sind, dann wird z.B. ein gesteuertes Patchmanagement schneller und effektiver funktionieren. In diesem Fall lohnt es sich, die Softwarekataloge zu sichten und Softwarereprodukte, die sich überlappen, neu zu bewerten und im besten Fall die Anzahl zu verringern. In diesem Untersuchungsprozess müssen auch die Anforderungen aus der IT-Security eine Rolle spielen. So können Entscheidungen gegen Produkte fallen, die zwar unternehmensintern akzeptiert sind und genutzt werden, die aber nicht mehr gepflegt werden und für die im schlimmsten Fall bereits Exploits zur Ausnutzung von Schwachstellen im Umlauf sind.

Je mehr Rechte zur Auswahl von Werkzeugen einer zentral arbeitenden Stelle gewährt werden, desto einfacher wird es sein, durch einen gesteuerten Einkauf die Anzahl unterschiedlicher Hard- und Softwarereprodukte zu minimieren.

5.5.7 Unterstützung des IT-Betriebs

Die IT-Security-Organisation ist im Allgemeinen nicht der Betreiber von IT-Systemen und kann damit technisch nicht dafür Sorge tragen, dass Informationen stets in einem vereinbarten Maß zur Verfügung stehen. Sie ist vielmehr in der Rolle des Anforderers zu sehen, die als möglichst unabhängige und objektiv auf den Betrieb schauende Instanz dafür Sorge trägt, dass die Schutzziele eingehalten werden. Im Kapitel »IT Business Continuity Management« werden die einzelnen Themenbereiche näher beleuchtet, die sich speziell mit der Verfügbarkeit beschäftigen. An dieser Stelle soll nur betont werden, welche Rolle die IT-Security-Organisation hinsichtlich der Verfügbarkeit spielt.

Parallel zum Betrieb steht der Manager IT-Security in der Verantwortung, die Umsetzung von Vorgaben zu überprüfen und im Fall von Abweichungen zu korrigieren. Dafür muss er einen Prozess initiieren, der dem Schema des Plan-Do-Check-Act-Zyklus folgt:



KAPITEL 5 – BETRIEB DER IT-SECURITY

- Die Anforderungen an den IT-Betrieb hinsichtlich des Schutzzieles Verfügbarkeit müssen definiert und durch die Unternehmensleitung abgesegnet werden.
- Mithilfe von Audits wird der aktuelle Status erfasst und durch den direkten Abgleich mit den Anforderungen bewertet.
- Maßnahmen werden festgelegt.
- Zu den Maßnahmen werden jeweils Kennzahlen definiert, die dazu dienen, den Umsetzungsgrad zu überwachen.



6 IT Business Continuity Management

6.1 Kapitelzusammenfassung

Das Business Continuity Management (ohne das führende »IT«) hat die Aufgabe, Strategien zu entwickeln, die große finanzielle Schäden vom Unternehmen abwenden. Diese werden sowohl präventiv als auch reaktiv angelegt. Ein Beispiel für ein präventives Instrument ist das Unternehmensrisikomanagement, das das finanzielle Risiko kommender Wechselkursschwankungen oder auch politischer Unruhen bewertet und entsprechende Maßnahmen empfiehlt. Als reaktiv zu bezeichnen sind wiederum Pläne in den Schubladen, die Werbemaßnahmen und Lobbyarbeiten beschreiben, die anzuwenden sind, falls das Unternehmen durch negative Schlagzeilen in der Presse auffällt und sich dies im Unternehmensergebnis niederschlägt. Das IT Business Continuity Management (nun mit der führenden Abkürzung »IT«) bedient aus Sicht der IT ebenfalls beide Perspektiven. Zum einen die Planungen für negative Ereignisse, die möglicherweise eintreten werden, als auch die stetige Vorsorge, IT-Systeme und damit die Verfügbarkeit von Daten auf einem möglichst hohen Niveau zu erhalten. Das IT Business Continuity Management (IT BCM) besteht damit primär aus den zwei Teilbereichen »IT-Notfallmanagement« und »Verfügbarkeitsmanagement«. Beide Bereiche nutzen gemeinsam Methoden zur Vorgehensweise wie z.B. die Business-Impact-Analyse und das IT-Risikomanagement.

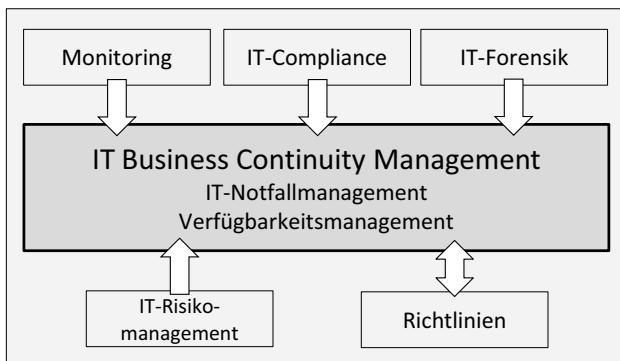


Abbildung 6.1: Primäre Abhängigkeiten von anderen Themen der IT-Security



Für die grundlegende Ausgestaltung eines funktionierenden BCM ist insbesondere das IT-Risikomanagement ein unverzichtbares Hilfsmittel. Aus diesem Grund ist es sinnvoll, sich zunächst die damit verbundenen Methoden in den entsprechenden Kapiteln anzuschauen.

Die Top-3-Fragen zum aktuellen Kapitel:

- Wird der Wert einzelner IT-Systeme für das Unternehmen ermittelt und dokumentiert? Der Wert ergibt sich dabei aus den Kosten, die bei Verlust der Verfügbarkeit der darüber verarbeiteten Daten entstehen würde.
- Ist eine praktikable Vorgehensweise zur Business-Impact-Analyse für die Ermittlung des Wertes von IT-Systemen beschrieben und veröffentlicht?
- Sind die Rahmenbedingungen, also der Anlass und die Art der Durchführung für beide Bereiche des IT Business Continuity Managements definiert und von der Unternehmensleitung abgesegnet?

6

6.2 Einführung

Neben dem Schutz von Vertraulichkeit und Integrität stellt die Sicherstellung der Verfügbarkeit von IT-Systemen und der darauf aufbauenden Arbeitsabläufen und Prozesse ein weiteres wichtiges Ziel und damit einen Eckpfeiler der IT-Security dar. Sowohl Disziplinen wie

- das IT-Notfallmanagement als auch
- die technischen Maßnahmen, die dazu dienen, Ausfallsicherheit zu gewährleisten, z.B. der Aufbau eines redundanten Rechenzentrums oder eines Serverclusters,

werden darunter zusammengefasst.

Beide Teilbereiche, siehe Abbildung 6.2, stützen sich maßgeblich auf die Methoden des IT-Risikomanagements und der Business-Impact-Analyse, um Prioritäten und Strategien festzulegen sowie Investitionsbudgets zielgerichtet einzusetzen zu können.

Der Begriff »IT Business Continuity Management« (IT BCM) hat sich gegenüber dem deutschen Ausdruck »Betriebliches Kontinuitätsmanagement in der IT« weitgehend durchgesetzt. Es beinhaltet Strategien, Pläne, Konzepte und handfeste Maßnahmen, die dazu dienen, den Ausfall betrieblicher Arbeitsab-



läufe und weitergefasst von Prozessen zu vermeiden, und falls er doch eintritt, Methoden anzubieten, diesen Ausfällen effektiv zu begegnen.

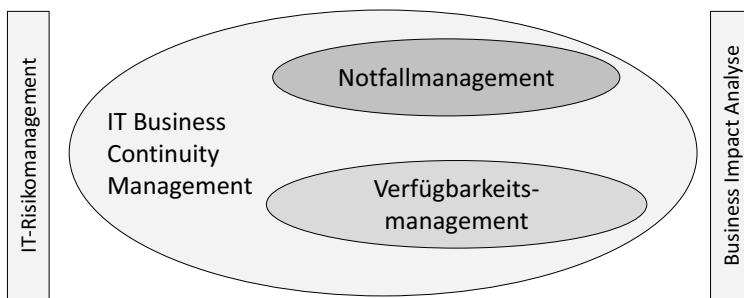


Abbildung 6.2: Bestandteile des IT BCM

6

Hinweis

Das IT Business Continuity Management (IT BCM) konzentriert sich als Teilbereich des Unternehmens-Business Continuity Managements auf diejenigen Arbeitsabläufe und Prozesse, die maßgeblich von IT-Systemen unterstützt werden.

Prozessereignisse übergeordneter Art wie z.B. der Wegfall eines wichtigen Kunden oder Lieferanten werden üblicherweise durch das Unternehmens-Business Continuity Management abgedeckt, während die Sicherstellung der Verfügbarkeit von Applikationen in den Bereich des IT BCM fällt. Vorhandene Schnittstellen, bedingt durch überschneidende Zielsetzungen, und eine ähnliche Vorgehensweise legen nahe, dass eine Zusammenarbeit zwischen den jeweiligen organisatorischen Einheiten, die sich auf verschiedenen Ebenen mit der Thematik BCM beschäftigen, lohnenswert ist. Als weiterer Grund spricht für eine enge Verzahnung, dass sich sowohl das betriebliche BCM als auch das IT BCM auf ein Risikomanagement stützen, das im Idealfall wiederum auf den gleichen Richtlinien und Methoden basiert.

Wie viele andere Bezeichnungen innerhalb einer fachspezifischen Terminologie ist auch der Begriff »IT Business Continuity Management« nicht eindeutig definiert. Im Rahmen des vorliegenden Buches wird der Ausdruck als Oberbegriff für alle Maßnahmen der IT und IT-Security genutzt, die der Sicherstellung des IT-gestützten Geschäftsbetriebs dienen. Zusammenge-



fasst dreht es sich um alle Maßnahmen, die dazu dienen, eine festgelegte oder vereinbarte Verfügbarkeit von IT-Systemen sicherzustellen.

In Anhang A.17 der ISO 27001:2013 wird das Thema unter der Überschrift »Information security aspects of business continuity management« aufgegriffen. Im Gegensatz zur Vorgängerversion dieser Norm wird das Thema weiter auf den Bezug zur IT-Security reduziert. Im Laufe der nächsten Jahre ist es damit gut möglich, dass sich allgemein das IT BCM von der Zuständigkeit in vielen Unternehmen weg von der IT-Security und vollständig hin zum operativen Betrieb der IT bewegen wird. Auf den ersten Blick erscheint dies auch offensichtlich sinnvoll zu sein, weil die Betriebsmannschaften letzten Endes die Verfügbarkeit der Systeme verantworten. Auf der anderen Seite argumentieren viele mittlere und größere Unternehmen, dass der Bereich IT-Security oder der Bereich Informationssicherheit für alle drei Schutzziele, zumindest was die Richtlinienkompetenz angeht, verantwortlich sein muss, da sie eng miteinander verzahnt sind. Spätestens, wenn die Verfügbarkeit aufgrund einer Schadsoftware eingeschränkt ist, weil sie dazu führt, dass die Arbeitsplatzrechner verschlüsselt werden, ist der direkte Bezug zu den Sicherheitsmaßnahmen bezüglich des Schutzzieles Vertraulichkeit offensichtlich. Dazu kommt das Argument der Unabhängigkeit. Ein Verantwortlicher für den Betrieb eines IT-Systems sollte nicht gleichzeitig festlegen können, inwieweit er für den möglichen Fall eines Ausfalls Vorsorge trifft. Vorsorge bedeutet auch immer Kosten und schmälert damit den Gewinn und letzten Endes den persönlichen Erfolg. In den IT-Grundschutz-Katalogen und dem BSI-Standard 100-4 wird das IT Business Continuity Management sehr pragmatisch auf das Thema »Notfallmanagement« reduziert.

Mit einiger Wahrscheinlichkeit wird sich der Ansatz des BSI mittelfristig durchsetzen. Die IT-Ziele werden von den Unternehmenszielen abgeleitet und das Gleiche gilt auch für die Rahmenbedingungen des IT BCM, die sich direkt auf die erforderliche Verfügbarkeit der Geschäftsprozesse bezieht. Damit wird der Handlungsspielraum der IT-Abteilung kleiner und damit fällt auch das Problem der fehlenden Unabhängigkeit weg. In ITIL gesprochen: Die IT bietet eine Dienstleistung an, der Attribute wie »Time to fulfill« oder eben auch die »Verfügbarkeit im Jahr« trägt. Das Rechenzentrum wiederum »erbt« die Anforderungen der Dienstleistung, die in diesem Rechenzentrum erbracht werden. Die IT-Security konzentriert sich dabei auf die Definition von Standards für die übergeordnete Aufgabe eines generellen Notfallmanagements.



Das führt heute zu einer stärkeren Gewichtung der IT-Security in Bezug auf diese Aufgabe, was sich unter anderem in der Hinzunahme der Gefährdung »Cyber-Angriff«, neben den üblichen Gefährdungen wie Feuer oder Erdbeben widerspiegelt.

Im Fokus des IT BCM liegen die wichtigen Geschäftsdaten und diejenigen IT-Systeme, die diese verarbeiten. Typische Notfälle sind davon abgeleitet Serverausfälle, Brände in Computerräumen, Fehler in der Benutzung von Applikationen oder der Ausfall von wichtigen Teilen der Infrastruktur. Im Rahmen des IT-Security-Managements sind je nach Aufstellung innerhalb des Unternehmens darüber hinaus auch nicht digitalisierte Informationen zu betrachten, wie sie z.B. in Karteikästen vorliegen oder in Ordnern in Papierform abgelegt sind.

Auch wenn die aktuelle ISO-Norm den Bezug zu den Kernaufgaben der IT-Security intensiviert und im gleichen Zug den weiter gefassten Bezug zum IT BCM reduziert, wird im Folgenden der oben beschriebene, umfangreichere Ansatz beschrieben. Aus diesem Grund wird nachfolgend die ISO 27001 der Version aus dem Jahr 2005 zusätzlich zu der aktuellen Version aufgeführt und in den weiteren Kapiteln auch als Basis genutzt.

Die folgende Aufstellung zeigt Maßnahmenziele, die Bestandteile eines IT BCM sein können:

- Die Verfügbarkeit der IT-Security-Maßnahmen zum Schutz von Vertraulichkeit und Integrität muss jederzeit gewährleistet sein. Das bezieht sich zum Beispiel auf den unterbrechungsfreien Betrieb von Sicherheitsarchitekturen, wie ein Patchmanagement oder auch die Überwachung der IT-Security durch ein Security Information and Event Management (SIEM).
- Es wird sichergestellt, dass die IT-Security in den Prozess zur Sicherstellung des Geschäftsbetriebs eingebunden ist.
- Es werden Standards definiert und Pläne zur Sicherstellung des Geschäftsbetriebs, die sicherheitskritisch sind, entwickelt, kommuniziert und umgesetzt. Ein Rahmenwerk führt die verschiedenen Dokumente zusammen und garantiert, dass alle Bestandteile jederzeit aktuell und verfügbar sind.
- Das Risikomanagement wird als Instrument zur Ausprägung und zur Priorisierung genutzt.



Hinweis

Die eben aufgeführten Maßnahmenziele bilden sowohl die Notfallvorsorge, die Kontinuitätsplanung, Techniken zur Überwachung der Systeme und die Prozesse für die Wiederherstellung nach Notfällen (Disaster Recovery) ab.

6

Der Aufbau eines IT BCM beinhaltet die Aufgaben, für die Zukunft zu planen und sich auf Ereignisse vorzubereiten, die vielleicht niemals eintreten werden. Da sowohl die dafür zu treffenden Annahmen als auch die daraus resultierenden Maßnahmen sehr individuell auf das jeweilige Unternehmen und die untersuchten Prozesse abgestimmt werden müssen, existiert kein umfassendes Softwareprodukt, das einem diese Arbeit komplett abnehmen könnte. Deshalb bedeutet es einigen individuell zu leistenden Aufwand, die richtige Vorgehensweise zu entwickeln. Augenmaß hinsichtlich der Kosten, Detailwissen auf technischer Ebene und ein hohes Maß an Koordinierungsaufwand sind die Schlüsselbausteine für ein funktionierendes IT BCM.

Im täglichen Leben machen wir alle BCM auf die eine oder andere Art und Weise. Dazu gehört der Ersatzreifen, der einen vor einer Reifenpanne schützen soll, genauso wie eine Vorsorgeimpfung gegen eine Krankheit, die hoffentlich niemals auftreten wird. Neben diesen Versicherungen, die uns im Notfall absichern sollen, ergreifen wir viele Maßnahmen, die vermeiden sollen, dass Notfälle überhaupt eintreten. Dazu gehören Tempolimits auf Straßen oder das Moskitonetz gegen Stechmücken, zusätzlich zum Mückenschutz, der auf die Haut aufgetragen wird, um sich gegen Krankheiten zu wappnen.

6.3 Abgrenzung der Begriffe

Nicht jeder Notfall ist eine Krise und eine Störung wird vermutlich nicht einmal in einem Notfallpapier Erwähnung finden. Spätestens, wenn der IT-Leiter vor der Frage steht, das Ausweichrechenzentrum zu aktivieren und infolge dessen in einem initialen Schritt alle aktiven Systeme herunterzufahren, wird er sich fragen, ob das in der gegenwärtigen Situation angebracht ist oder nicht. Schlussendlich wird jemand eine solche Entscheidung treffen müssen, hilfreich ist aber in jedem Fall eine klare Definition, was ein Notfall ist, wann



es sich um eine Krise handelt und wann welcher Plan zum Einsatz kommt. Aus diesem Grund grenzen wir vier verschiedene Härtegrade voneinander ab: die einfache Störung, den Notfall, die Krise und die Katastrophe. In den meisten Unternehmen werden die ersten drei Kategorien gelebt. Die Katastrophe fällt aus einem bestimmten Grund aus der Reihe, sie ist für viele Unternehmen schlicht zu groß, um geeignete Maßnahmen definieren, trainieren und auch bezahlen zu können.

- **(Einfache) Störung:** Hierbei handelt es sich um die typischen Meldungen bei der Hotline. Ein Mail-Programm funktioniert nicht mehr oder ein Rechner lässt sich nicht starten. Für diese Fälle setzen Unternehmen Ticketsysteme ein und schulen die Mitarbeiter am Telefon per Knowledge-Datenbanken, in denen eine Vielzahl von möglichen Problemen bereits beschrieben ist – inklusive Lösungsweg.
- **Notfall:** Hinter einem Notfall steckt im Allgemeinen nicht mehr ein Endgerät eines Benutzers, sondern ein wichtiges IT-System, dessen Ausfall erhebliche monetäre Auswirkungen haben kann, falls dieser nicht schnell behoben wird. Ein Notfall kann nicht mehr an der Hotline bearbeitet werden und wird spätestens von dort an den Systembetreiber eskaliert. Hier setzt das IT-Notfallmanagement an. Je nach Schweregrad werden die im Notfallhandbuch beschriebenen Register gezogen.
- **Krise:** Die Krise unterscheidet sich vom Notfall vor allem darin, dass sie im Notfallprozess nicht vorgesehen ist und ein Risiko mit sich bringt, das bis zur Existenzgefährdung des Unternehmens reichen kann. Hier setzen Maßnahmen wie das Herauffahren eines Cold-Standby-Rechenzentrums an. Die aktiven Systeme sind nicht zeitnah wiederherzustellen, also weicht man auf parallel arbeitende Strukturen aus. Dabei kann es sich auch um einen Standby-Cluster in einem anderen Gebäude handeln.
Eine Krise kann auch ein Cyber-Angriff sein, der die gesamte Produktion lahmlegt. In diesem Fall wird zumindest die Polizei eingeschaltet, und wenn das Unternehmen nicht über eine entsprechende Abteilung verfügt, die genau für diesen Fall ausgebildet ist, werden externe Forensiker, Spezialisten zum Thema Produktions-IT etc. herangezogen.
- **Katastrophe:** Die Katastrophe ist vom Unternehmen selbst nicht mehr alleine zu bewältigen. Eine Katastrophe kann dabei ein Erdbeben sein oder auch eine Überschwemmung. In diesen Fällen gilt das erste Augenmerk dem Schutz der Mitarbeiter, und die Datenverarbeitung rückt in der Priorisierung zurück.



ritätenliste nach hinten. Entscheidend ist die nahtlose Zusammenarbeit zwischen den eigenen Mitarbeitern und externen Organisationen wie der Polizei, der Feuerwehr, dem Technischen Hilfswerk und weiteren Hilfsorganisationen.

Schon die Krise ist nicht mehr durch die IT-Abteilung im Alleingang zu bewältigen. Dies wird deutlich, wenn man ein typisches IT-Problem betrachtet, einen Angriff durch Computerviren. Fallen dadurch bedingt Produktionsrechner aus und steht die Produktion, zum Beispiel weil die Rechner verschlüsselt werden, dann sollte ein solcher Vorfall nicht mehr alleine durch die IT bearbeitet werden. Dafür ist ein Krisenstab zuständig, der sich um die gesamte Bandbreite des Problems kümmern kann und der auch die erforderliche Kompetenz hat, dies zu tun. Das beginnt beim Anruf bei der Polizei, unter Umständen der Benachrichtigung des Versicherungsunternehmens, mit dem eine sogenannte Cybercrime-Versicherung abgeschlossen wurde, natürlich der Einbezug der IT-Abteilung und der IT-Security, die Kontaktaufnahme mit dem Lieferanten der Rechner und endet vielleicht beim Kauf von Bitcoins, um ein Passwort zur Entschlüsselung der Rechner zu erwerben.

6

6.4 IT-Notfallmanagement und Verfügbarkeitsmanagement

Das IT-Notfallmanagement kommt dann zum Tragen, wenn ein IT-System ausfällt, Daten nicht wie benötigt zur Verfügung stehen oder ein Prozess nicht das geforderte Ergebnis liefert.

Das Verfügbarkeitsmanagement (*availability management*) ergänzt diese reaktiven Prozesse durch Maßnahmen, die den allgemeinen Grad an Verfügbarkeit erhöhen. Zu diesen Maßnahmen gehören eine Reihe von technischen und organisatorischen Maßnahmen, zu denen unter vielen anderen die klassischen Themengebiete wie die Datenspiegelung, die Datensicherung oder der Aufbau kompletter redundanter Systeme oder im Extremfall der Aufbau redundanter Rechenzentren gehören.

Wie aus Abbildung 6.2 ersichtlich wird, teilen sich beide Unterbereiche des IT BCM die Methoden des IT-Risikomanagements und der Business-Impact-Analyse.



6.5 Gesetzliche Rahmenbedingungen des IT Business Continuity Managements

Die Geschäftsführung und der Vorstand eines Unternehmens haben dafür Sorge zu tragen, dass der Geschäftsbetrieb störungsfrei verläuft. Zudem müssen Vorkehrungen getroffen werden, dass Störungen frühzeitig erkannt und gegebenenfalls behoben werden. Dieser nachvollziehbar wichtige Grundsatz wird unter anderem im Art. 91 des Aktiengesetzes (AktG) deutlich formuliert, der als Ergänzung zu den allgemeinen Bestimmungen des § 317 Abs. 2 des Handelsgesetzbuchs dient.

In Art. 91 des AktG wird weiter ausgeführt: »Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.« Die Verpflichtung der Unternehmensführung wird in Art. 93 des AktG durch das Prinzip der »Haftung des Vorstands« ergänzt.

Aus diesen Vorgaben sind analog zu den Maßnahmenzielen der ISO 27001 viele Aufgaben ableitbar, die ein Unternehmen hinsichtlich des IT BCM abarbeiten muss. Die Sicherstellung des störungsfreien Betriebs weist auf das Sicherheitsziel Verfügbarkeit und die technischen Maßnahmen hin, die im Rahmen des Verfügbarkeitsmanagements anstehen. Weitere Maßnahmen sind die Überwachung durch das Monitoring und die Implementierung eines IT-Notfallmanagements, um auf Krisen adäquat reagieren zu können.

6.6 Business-Impact-Analyse

Die Aufgabe der Unternehmens-IT ist es, den externen oder internen Kunden Dienstleistungen zu erbringen. Dienstleistungen in diesem Sinne reichen von der Bereitstellung von Speicherplatz über die Installation und den Betrieb von Softwareprodukten bis hin zur Beratung bei Projekten. Von diesen Dienstleistungen hängt ein Großteil der betrieblichen Prozesse ab. So kann der Ausfall eines Druckers zum Ausdruck von Barcodes bereits den Produktionsprozess oder Auslieferungsprozess von Produkten behindern.

Hinweis

Nicht jeder unterstützte Prozess ist indes gleichermaßen wichtig, und davon abgeleitet ist auch nicht jede Dienstleistung der IT und jedes IT-



System, das für die Sicherstellung der Dienstleistung sorgt, gleich hoch zu priorisieren.

Die Aufgabe der Business-Impact-Analyse (BIA) ist es, zu ermitteln, inwieweit der Ausfall eines IT-Systems Einfluss auf den Betrieb von Geschäftsprozessen hat. Aus Sicht der IT-Security gilt es zu ermitteln, welche IT-Systeme für welche kritischen Geschäftsprozesse erforderlich sind, um für genau diese Systeme priorisiert Notfallpläne zu erstellen.

Wichtig

6

Nicht in jedem Fall ist es erforderlich, eine vollständige oder komplett formale BIA durchzuführen. Ist ein Unternehmen ausreichend übersichtlich strukturiert, dann ist das Wissen darüber, was wichtig ist und besonders vor dem Ausfallen geschützt werden muss, bereits in den Köpfen der Mitarbeiter vorhanden und muss nur notiert werden.

Für die Durchführung einer BIA sind umfangreiche Kenntnisse der relevanten Prozesse im Unternehmen, deren Abhängigkeiten voneinander und die unterstützenden IT-Systeme erforderlich. In den meisten Fällen ist dieses Wissen weder bei dem Manager IT-Security noch bei den Mitarbeitern der IT in ausreichendem Maß vorhanden. Aus diesem Grund werden die Verantwortlichen aus den Fachbereichen hinzugezogen, die in diesem Fall auch die Verantwortung für die Priorisierung der Prozesse und die Klassifizierung der Assets übernehmen. In letzter Instanz obliegt es der Unternehmensleitung, die Gesamtaufstellung abzunehmen und damit als Grundlage für das IT-Notfallmanagement zu bestätigen.

6.6.1 Erfassung und Priorisierung der Geschäftsprozesse

Um sich nicht in einer Vielzahl von zu analysierenden Prozessen und davon abgeleiteten Systemen zu verlieren, gilt es zunächst, sich einen Überblick über alle wichtigen, im Unternehmen betriebenen Prozesse zu verschaffen. Prozesse im Sinne der Business-Impact-Analyse sind definierte Arbeitsabläufe, die wiederum aus Einzelschritten bestehen. Die Definition, ab wann ein Vorgang als Arbeitsablauf, Teilprozess oder Prozess bezeichnet wird, ist stark von



der Methodik der unternehmerischen Prozessplanung abhängig und sollte in jedem Fall festgelegt sein, bevor die Business-Impact-Analyse durchgeführt wird.

Arbeitsabläufe in einem Unternehmen werden immer den Zweck haben, Ziele des Unternehmens direkt, auf welcher Ebene auch immer, oder aber indirekt durch Unterstützung weiterer Prozesse zu erreichen. Daraus folgt, dass die Definition von Prozessen zunächst einmal ohne Betrachtung der IT oder der IT-Strategie erfolgt. Die IT ist in diesem Fall der Dienstleister, der entsprechende unterstützende Systeme zur Verfügung stellt und auch verantwortet. Des Weiteren kann man davon ableiten, dass der Personenkreis, der die Geschäftsprozesse ermittelt, nicht unbedingt aus der IT kommen sollte, sondern vielmehr mit den Unternehmenszielen und den Konsequenzen, die bei Nichterreichung anfallen, vertraut sein muss.

Die Herausforderungen, denen dieser Personenkreis gegenüberstehen wird, können erdrückend groß werden. Dies geschieht zumeist dann, wenn Prozesse zu detailliert dargestellt werden und die sich daraufhin ergebende, aufgeblasene Darstellung so unübersichtlich wird, dass eine Visualisierung nicht mehr sinnvoll stattfinden kann. In diesen Fällen wächst das Vorhaben schnell zu etwas heran, das nicht bis zum Ende durchgehalten wird bzw. letztendlich nicht gepflegt werden kann.

Hinweis

Die Hauptaufgabe besteht darin, einen Kompromiss zwischen Detailtiefe und Nutzbarkeit zu schaffen. Es ist also wichtig, eine Person im Boot zu haben, die Entscheidungen treffen kann, die dafür sorgen, dass die Ergebnisse sowohl ausreichend detailliert, aber auch pragmatisch genug sind. Ein Probelauf mit einem kleinen, überschaubaren Prozess zeigt häufig bereits die Herausforderungen auf, ohne sich gleich zu verrennen.

Phase 0: Erfassung und Darstellung der Geschäftsprozesse

Der erste Schritt und die wichtigste Ausgangsvoraussetzung ist das Vorhandensein einer möglichst vollständigen Übersicht aller wichtigen Geschäftsprozesse. Das Wort »wichtig« ist naturgemäß frei für jede Art der Interpretation. Als Anhaltspunkt kann eine Liste dienen, die die fünf bis maximal zehn der



von der Unternehmensleitung als am kritischsten eingestuften Prozesse identifiziert. Diese Liste kann als generelle Ausgangsliste angesehen werden, und es ist sinnvoll, mit dem Prozess aus der Liste zu beginnen, der am wenigsten komplex zu sein scheint. Sind die Business-Prozesse zu komplex oder zu allgemein gehalten, wie z.B. ein Prozess »Produktion«, dann ist es erforderlich, diesen wiederum in Unterprozesse zu gliedern. In diesem Fall könnte man die Produktion je Produktionsstandort betrachten oder aber einen Teilaspekt, der für alle Standorte gelten kann, wie »Softwareunterstützung der Logistik«.

Im Rahmen des Gesamtprojekts wird für jeden Prozess aus der Liste eine Business-Impact-Analyse durchgeführt. Zusätzlich zu den Prozessen ist es wichtig zu wissen, wo die grundlegenden Daten des Unternehmens liegen, um geeignete Querverbindungen zu den Prozessen aufbauen zu können.

6

Für die Visualisierung von Prozessen bietet es sich an, die jeweiligen Einzelaktivitäten, aus denen der Gesamtprozess zusammengesetzt ist, in Form eines Flussdiagramms abzubilden. Dadurch lassen sich auch Abhängigkeiten von Prozessen aufzeigen. In Fall von Abhängigkeiten von Prozessen untereinander wird der Output von vorgesetzten Prozessen als Input von nachgeordneten Prozessen dargestellt.

Folgende Informationen sollten für jeden Prozess erfasst werden:

- eine eindeutige Bezeichnung für den Prozess
- eine Beschreibung und Einordnung in den Unternehmenskontext
- Name und Abteilung des Prozessverantwortlichen
- Name und Abteilung derjenigen Person, die die Kritikalität und die Service Level Agreements festlegt
- die Abhängigkeit von einem vorgesetzten Prozess inklusive des Dateninputs
- die Voraussetzung für einen nachgesetzten Prozess inklusive des Datenoutputs
- den Grad der Abhängigkeit der Geschäftsprozesse untereinander

Phase 1: Vorauswahl der Geschäftsprozesse

Ziel des zweiten Schritts ist es, eine priorisierte Liste der wichtigsten Prozesse anzufertigen und dabei weniger wichtige Prozesse auszusondern. Dies ist



erforderlich, um sich nicht ob der schieren Anzahl an Prozessen von vornherein zu verzetteln.

Viele Prozesse innerhalb eines Unternehmens können stunden- oder sogar tagelang teilweise oder vollständig ausfallen, ohne dass die vorgegebenen Ziele deshalb verfehlt werden. Häufig ist dies bei Prozessen der Fall, für die Ausweichprozeduren existieren. Ein klassisches Beispiel ist die Datenerfassung. Fällt die automatisierte, elektronische Datenerfassung aus, so werden die Daten vorübergehend manuell erfasst. Da durch die Nacherfassung zu einem späteren Zeitpunkt trotzdem zusätzliche Kosten entstehen, ist es natürlich erforderlich, auch diese Prozesse zu betrachten und entsprechende Handlungsvorgaben zu erstellen.

Phase 2: Schadensanalyse

6

Grundlage für die Schadensanalyse sind die entstehenden Kosten, wenn der zu beurteilende Prozess die gesteckten Ziele nicht erreicht. Die Schadensanalyse wird häufig gestaffelt, um aufzuzeigen, welche Kosten nach wie langer Ausfallzeit auftreten. So kann es vorkommen, dass es unproblematisch ist, wenn ein Prozess für eine Stunde ausfällt, der Ausfall über einen Zeitraum von 24 Stunden aber existenzielle Probleme hervorrufen würde. Einheitliche Bewertungskriterien müssen im Vorfeld definiert sein, um die Ergebnisse der Schadensanalyse vergleichbar zu gestalten.

Phase 3: Festlegung Prozess Service Level Agreements

Von den Ergebnissen aus Phase 2 ausgehend werden nun die Wiederanlaufparameter jedes Prozesses festgelegt. Dazu gehören zunächst die Parameter, die aus Service Level Agreements bekannt sind:

- Maximal tolerierbare Ausfallzeit (z.B. 1 Stunde, 4 Stunden, Arbeitstag, 24 Stunden) auf Basis formal festgelegter Parameter, um die Vergleichbarkeit zwischen Prozessen zu gewährleisten
- Das minimale Wiederanlaufniveau, das erforderlich ist, um zumindest einen Notbetrieb aufrechterhalten zu können

Phase 4: Berücksichtigung von Abhängigkeiten

Je größer ein Unternehmen ist, je mehr Produkte es vertreibt oder produziert, abhängig von der organisatorischen Aufstellung und je nachdem wie die



interne Dienstleistungsstruktur aufgebaut und gegliedert ist, sind die bestehenden Prozesse mehr oder weniger stark voneinander abhängig. In manchen Unternehmen sind im Zuge der Digitalisierung große Teile der IT in kleine Dienstleistungseinheiten fragmentiert worden, die auf komplexe Weise miteinander agieren – entweder parallel zueinander oder auch seriell. Die serielle Vorgehensweise wird dabei überwiegen und das bedeutet, dass der Output von Prozess A der Input von Prozess B ist. In diesem Fall kann nicht mehr jeder einzelne Prozess isoliert betrachtet werden. Um dieser Tatsache Rechnung zu tragen, müssen diese Prozesse so dokumentiert werden, dass ihre logische Verknüpfung sichtbar wird.

6

Je mehr ein Prozess von einer übergeordneten Ebene aus betrachtet wird, desto seltener werden Abhängigkeiten vorkommen. Mit anderen Worten: Prozesse, die mehr Arbeitsschritte bzw. Teilprozesse beinhalten, werden zwar komplexer, auf der anderen Seite aber auch unabhängiger von anderen Prozessen. Ein typisches Beispiel wäre der »Bestellprozess«. Splittet man ihn in die Prozesse »Bestellung elektronisch aufgeben« und »Wareneingang« auf, so würde der Ausfall des ersten Prozesses für zwei Arbeitstage automatisch auch den zweiten Prozess behindern – ohne dass der Wareneingang ausgefallen wäre. Im Falle dieses Ausfalls wäre es nun erforderlich, eine direkte Beziehung zwischen diesen beiden Prozessen darzustellen, um sicherzustellen, dass die entsprechenden Verantwortlichen für beide Prozesse parallel über die Situation benachrichtigt werden. Wird nur ein Prozess mit dem Namen »Bestellung und Wareneingang« definiert, so ist die Abhängigkeit in sich gegeben.

Phase 5: Priorisierung der Geschäftsprozesse

In vielen Fällen ist es selbst in größeren Unternehmen sinnvoll, die Anzahl der Top-Prozesse auf fünf bis zehn Kernprozesse zu beschränken. Für diese kritischen Geschäftsprozesse ist es erforderlich, ein vollständiges IT-Notfallmanagement durchzuführen. Für alle weiteren Prozesse reicht es meistens, auf wenigen Seiten Handlungsanweisungen zusammenzutragen, die dazu dienen, den Ausfall dieser Prozesse zu überbrücken oder auf andere Prozesse auszuweichen.

In dieser Phase werden alle Prozesse, die nicht bereits in Phase 1 ausgesondert wurden, mithilfe der Schadensanalyse aus Phase 2 und den definierten Wie-



deranlaufkriterien aus Phase 3 priorisiert. Die am höchsten bewerteten Prozesse sind diejenigen, die für die Kernaufgaben des Unternehmens kritisch sind, und werden als »Kernprozesse« oder »kritische Prozesse« bezeichnet.

Kernprozesse müssen nicht für das gesamte Unternehmen definiert werden. Es kann genauso gut sinnvoll sein, Kernprozesse für jeden Standort einzeln zu definieren. Dies ist zum Beispiel dann der Fall, wenn ein Standort produziert, ein Standort die Verwaltung beherbergt und ein weiterer für den Vertrieb zuständig ist. Die Kernprozesse werden in diesem Fall für jeden Standort völlig unterschiedlich aussehen. Ist im Vertriebsstandort das Telefon noch ein sehr wichtiger Faktor, so spielt es im Produktionsstandort vermutlich eher eine untergeordnete Rolle.

Prozesse, die zunächst nicht als kritisch definiert wurden, können dennoch dann kritisch sein, wenn Kernprozesse von ihnen abhängig sind. Dies kann z.B. der Fall sein, wenn ein Prozess Daten erzeugt, die in einen Kernprozess einfließen und von denen der korrekte Ablauf des Kernprozesses abhängig ist.

6

Phase 6: Zuordnung von Werten

Im Rahmen des IT Business Continuity Managements werden Prozesse betrachtet, die von IT-Systemen unterstützt werden. So ist der Bestellprozess beispielsweise unter anderem von einer Bestellsoftware, von einer internen und eventuell auch externen Netzwerkverbindung und einem Datenspeicher abhängig. In Phase 6 werden für jeden Prozess diejenigen Unternehmenswerte (*assets*) aufgeführt, die für das Funktionieren des jeweiligen Prozesses erforderlich sind. Unter Werten versteht man in diesem Fall technische Systeme und Daten, aber auch Büromaterial oder Räumlichkeiten.

Dieser Schritt kann naturgemäß sehr viel Dokumentation erzeugen, die entsprechend gut aufgebaut werden muss. Aus diesem Grund ist zu empfehlen, dass er zunächst nur für die am höchsten priorisierten Prozesse durchgeführt wird.

Phase 7: Festlegung Asset Service Level Agreements

Der letzte Schritt ist gleichzeitig auch der aufwendigste. Konsequenterweise werden nun für alle in Phase 6 erfassten Werte die Klassifizierung und die Wiederanlaufzeiten bestimmt.



- Maximal tolerierbare Ausfallzeit des Werts (z.B. 1 Stunde, 4 Stunden, Arbeitstag, 24 Stunden) auf Basis formal festgelegter Parameter, um die Vergleichbarkeit zwischen Werten zu gewährleisten.
- Klassifizierung des Werts auf Basis der Wichtigkeit für den zugrunde liegenden Prozess.

6.6.2 Business-Impact-Analyse in der Praxis

Der Aufwand für den Aufbau und die Pflege des IT-Notfallmanagements hängt direkt von der Anzahl an erfassten und als kritisch bezeichneten Prozessen ab. Jeder zusätzliche Prozess definiert neue IT-Systeme, die wiederum gegen Ausfall geschützt oder deren Ausfall durch die Erzeugung von Notfallmaßnahmen minimiert werden muss. Der dadurch erzeugte Aufwand ist nicht als Einmalaufwand zu sehen. Die Pflege und stetige Weiterentwicklung der verschiedenen Dokumentationen ist eine laufende Aufgabe, die Ressourcen benötigt. Je höher der Aufwand, desto höher die Kosten und umso schwerer wird es sein, diese zu verargumentieren und der Unternehmensleitung plausibel zu machen. Die Unterstützung der Unternehmensleitung wiederum ist eine Erforderlichkeit, ohne die kein IT-Notfallmanagement möglich ist, die nichts anderes darstellt als eine Versicherung, die für eventuell eintretende Probleme in der Zukunft gedacht ist. Auf der anderen Seite dürfen kritische Prozesse nicht ignoriert werden, um im Notfall keine immensen Kosten zu verursachen. Dieser Spagat ist der Pfad, auf dem sich der Manager IT-Security bewegt, wenn er ein IT BCM einführen bzw. erweitern möchte.

6

Hinweis

Die Aufgabe des Managers IT-Security innerhalb des Prozesses der BIA liegt naturgemäß eher in der Moderation denn in der tatsächlichen Bewertung. Zum Ziel dieser Moderation gehört auch eine praxisnahe Umsetzung der doch sehr theoretischen Inhalte. So werden die verschiedenen Stufen der BIA in sehr wenigen Unternehmen bis ins Detail umgesetzt werden. Vielmehr baut man auf die Erfahrungen der an der Diskussion beteiligten Mitarbeiter und auf die mit der Zeit wachsende Routine bei der Bewertung. Nichtsdestotrotz sollte ein Manager IT-Security die grundsätzlichen Teilgebiete kennen, um eine Bewertung der Nützlichkeit einer durchgeföhrten BIA beurteilen zu können.



6.7 Weitere Einflussfaktoren

Unter Zuhilfenahme der Business-Impact-Analyse werden die kritischen Geschäftsprozesse analysiert und die dafür erforderlichen Systeme und Unternehmenswerte identifiziert. Die nun folgende Risikoanalyse dient dazu, diejenigen Risiken zu ermitteln und zu bewerten, die die Verfügbarkeit dieser Systeme und damit die Geschäftsprozesse gefährden. Das IT-Notfallmanagement wird dann die Aufgabenstellung verfolgen, Notfallpläne, Wiederanlaufpläne etc. bereitzustellen, um diesen Gefahren zu begegnen. Der Schritt der Risikoanalyse und Risikobewertung verfolgt damit das Ziel einer weiteren Priorisierung, welche Systeme zunächst betrachtet werden sollten, und der Ermittlung, gegen welche Gefährdungen sie zu schützen sind.

Weitergehende Informationen zum Thema Risikomanagement finden Sie im entsprechenden Kapitel.

Neben den IT-Risiken, die zunächst im Umfeld von IT-Systemen zu suchen sind, gibt es zahlreiche weitere mögliche Risikofelder, die im Rahmen eines übergeordneten Unternehmensrisikomanagements bearbeitet werden. Der Prozess »Wareneinkauf« hängt beispielsweise nicht nur an den unterstützenden IT-Systemen, sondern u.a. auch an dem Risiko »Lieferant ist nicht mehr verfügbar«. Ein IT-Risikomanagement wird dieses neue Risiko nicht erfassen und dementsprechend auch keine Notfallstrategie dafür entwickeln. Daraus folgt, dass es in vielen Fällen sinnvoll ist, zumindest Verknüpfungen zur Datenbasis des Unternehmensrisikomanagements herzustellen und in die Risikoanalyse zumindest mit einzubeziehen. Dabei ist es sehr hilfreich, wenn die Prozesserfassung analog zur Erfassung durch das Unternehmensrisikomanagement erfolgt.





7 IT-Notfallmanagement

7.1 Kapitelzusammenfassung

Der erste Teilbereich des IT Business Continuity Managements, der hier behandelt werden soll, ist das IT-Notfallmanagement, der zweite Bereich folgt im nächsten Kapitel unter der Überschrift »Verfügbarkeitsmanagement«. Beim IT-Notfallmanagement handelt es sich um ein Paket an Prozeduren und Dokumenten, die im Vorfeld erstellt werden, um im Notfall herangezogen und umgesetzt werden zu können. Das Ziel ist hier, mit möglichst wenig Zeitverlust und unter möglichst geringen Datenverlusten den Normalzustand wiederherzustellen. Falls möglich, ganz im Sinne des kontinuierlichen Verbesserungsprozesses, soll aus jedem Notfall zudem die Lehre gezogen werden, wie man den Notfall beim nächsten Mal vermeidet oder zumindest die Auswirkungen verringern kann.

Die Top-6-Fragen zum aktuellen Kapitel:

- Sind die kritischen IT-Systeme und Applikationen bekannt?
- Sind die Begriffe Störung, Notfall und Krise definiert und ist die Alarmierungskette korrekt implementiert?
- Sind die Mitglieder der IT-Notfallteams benannt? Sind die einzelnen Rollen zugeordnet und die Zuständigkeiten definiert?
- Existieren für die kritischen IT-Systeme Anleitungen für die Wiederherstellung?
- Existieren Notfallprozeduren, die die Vorgehensweise im Notfall skizzieren?
- Werden IT-Notfälle simuliert und die Reaktion darauf geprobt?

7.2 Einführung

Das IT-Notfallmanagement ist Bestandteil des IT Business Continuity Managements und hat die grundsätzliche Aufgabe, Methoden und Maßnahmen bereitzustellen, die zur schnellen Lösung einer Notfall- oder Krisensituation dienen.



Das IT-Notfallmanagement ist ein Sammelbegriff für alle Schritte von der Notfallvorsorge zu den Notfallübungen über den Notbetrieb bis hin zur Bewältigung eines Notfalls. Es umfasst die Definition von Verantwortlichkeiten, die Erstellung und Pflege von Notfallplänen und aller Maßnahmen, die im Rahmen von Notfällen abzuarbeiten sind.

7.3 IT-Notfallmanagement

Die Ziele des IT-Notfallmanagements basieren auf den Richtlinien, die die Unternehmensleitung hinsichtlich des Business Continuity Managements (BCM) und davon abgeleitet des IT Business Continuity Managements festlegt. Die dort beschriebenen Zielsetzungen und Aufgaben werden durch eine Notfallorganisation abgearbeitet und umgesetzt.

7

Die grundsätzliche Vorgehensweise, ein IT-Notfallmanagement aufzubauen und zu betreiben, ist in Abbildung 7.1 dargestellt. Auch in diesem Fall handelt es sich um einen sich ständig wiederholenden Regelkreis.

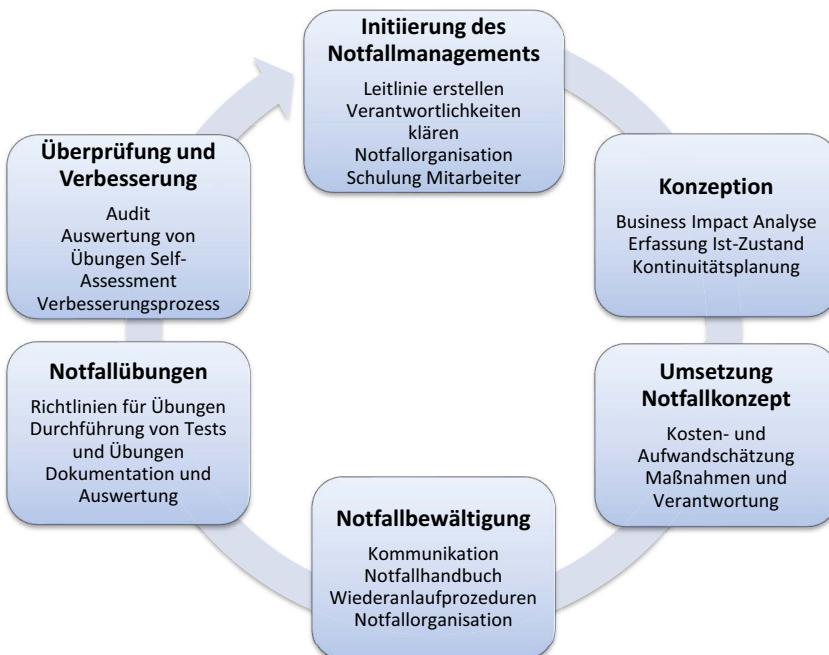


Abbildung 7.1: IT-Notfallmanagement nach BSI-Standard 100-4



Mit der Ableitung der Ziele und Aufgaben aus der BCM-Richtlinie beginnt der Regelkreis. Anhand der Zielvorgaben werden im Folgenden die Umfänge und die Leistungen des IT-Notfallmanagements direkt abgeleitet.

Während der Konzeption werden Basisdaten ermittelt, die wiederum erforderlich sind, um die Methoden, Maßnahmen und die Dokumentationen zielgerichtet definieren zu können. Die Erfassung der beteiligten Prozesse und IT-Systeme im Rahmen der Business-Impact-Analyse nimmt dabei eine herausragende Stellung ein. Sobald die Festlegung steht, um was sich das IT-Notfallmanagement kümmern soll, folgen die weiteren Schritte der Ausarbeitung von Handbüchern, der Ausgestaltung einer Notfallorganisation und die Festlegung der weiteren Maßnahmen. Übungen und die Einarbeitung daraus gewonnener Erfahrungen runden die Konzepte im Zuge des Regelkreises weiter ab.

7.4 Richtlinie zum IT-Notfallmanagement

Die Stellung des IT-Notfallmanagements innerhalb eines Unternehmens spiegelt sich in den gesetzlichen Anforderungen wider. Demzufolge ist die Festlegung, dass es ein solches geben muss und wie dieses grundsätzlich auf strategischer Ebene auszugestalten ist, Aufgabe der Unternehmensleitung. Die Erforderlichkeit zur Einführung und zum Betrieb eines IT-Notfallmanagements und die Rahmenbedingungen, unter denen es ausgestaltet wird, spiegeln sich in der Richtlinie zum IT-Notfallmanagement wider. Als Dokument der obersten Ebene verliert es sich nicht in technischen Details und hat als Zielpublikum alle Parteien innerhalb des Unternehmens im Blick, die Daten verarbeiten, Daten erzeugen oder die auf Dienstleistungen angewiesen sind, die ohne die Verfügbarkeit von Daten und Applikationen nicht erbracht werden können.

Ein effektives IT-Notfallmanagement ist von einer Vielzahl unterschiedlicher Organisationseinheiten abhängig, und demzufolge ist es wichtig, darauf zu achten, dass die Richtlinie von allen Beteiligten verstanden und akzeptiert wird.

Folgende Punkte sollte eine solche Richtlinie zumindest beinhalten:

- Eine genaue Definition des Begriffs IT-Notfallmanagement
- Eine klare Aussage, dass es Teil der Unternehmensstrategie ist, durch ein etabliertes IT-Notfallmanagement die Verfügbarkeit von Unternehmens-



daten sicherzustellen. An dieser Stelle ist es sinnvoll, herauszustellen, dass die Unternehmensleitung Auftraggeber der Richtlinie und damit der gesamten Thematik ist. Häufig wird in diesem Zusammenhang auch erwähnt, welche Organisationseinheit für die Ausgestaltung der Richtlinien und welche für die Umsetzung verantwortlich ist. Das wird in den meisten Fällen neben der operativen IT auch die IT-Security-Organisation sein.

- Die Ziele des IT-Notfallmanagements. Für welche IT-Systeme, Prozesse und Daten sollen welche Anforderungen erfüllt werden. Dieser Punkt baut bereits auf einer Priorisierung von Prozessen auf, wie sie nach Durchführung einer Business-Impact-Analyse vorliegt. Dieser Punkt kann auch auf ein verlinktes Dokument verweisen, da die entsprechenden Inhalte regelmäßig angepasst werden müssen und damit im Gegensatz zu den anderen Punkten der Richtlinie weniger statisch sind.
- Die gesetzlichen oder normativen Modelle, auf denen das IT-Notfallmanagement aufbaut und die zu beachten sind. Dadurch wird gleichzeitig der Rahmen für den Aufbau des IT-Notfallmanagements vorgegeben.
- Der Link zu den korrespondierenden Dokumenten aus dem Bereich des Datenschutzes. Hier ist zu dokumentieren, welche Maßnahmen getroffen werden, um die Verfügbarkeit und Belastbarkeit von IT-technischen Systemen zu gewährleisten, die personenbezogene Daten verarbeiten.

Nach der Erstellung der Richtlinie muss diese adäquat innerhalb des Gelungsbereichs, also zumindest in der IT-Abteilung kommuniziert werden. Alle weiteren Richtlinien zu diesem Thema bauen im Wesentlichen auf den hier definierten Grundsätzen auf und leiten ihre Legitimation von dieser ab, was wiederum die Wichtigkeit der Richtlinie betont.

7.5 Ableitung von Notfallstrategien

So verschieden Notfälle sind, so verschieden sind auch die Strategien, mit denen darauf reagiert wird. Bevor also eine Strategie bewusst ausgewählt wird, ist es immer wichtig, auf die vorliegenden Daten zu achten, die im Zusammenhang mit den betroffenen IT-Systemen, Prozessen und Daten vorliegen. Auf Basis der Business-Impact-Analyse wurden die kritischen Geschäftsprozesse erfasst und die jeweilige Priorität festgelegt. Die damit verbundenen Service Level Agreements legen fest, für welchen Zeitraum der Ausfall eines Prozesses akzeptabel ist. Zudem sind die Kosten hinterlegt, die ein vollständiger



oder teilweiser Ausfall verursachen würde. Welche Risiken für den Betrieb der kritischen Prozesse bestehen, wie die Wahrscheinlichkeit für deren Eintritt aussieht und welche Kosten bei einem Notfall auflaufen würden, wurde im Rahmen der Durchführung eines IT-Risikomanagements erklärt. Alle diese Parameter können Einfluss auf die Krisenreaktion haben und Einfluss auf die umfassende Strategie, häufig Kontinuitätsstrategie genannt, nehmen.

Die Anzahl an vorab erarbeiteten Strategien, deren Komplexität und damit der Aufwand, den die Erstellung und Pflege generiert, sollten immer in das Verhältnis mit dem zu erwartenden Nutzen gestellt werden. Dabei gilt der Grundsatz, dass je wichtiger der Prozess ist, desto mehr Aufwand wird auch in die Risikovorbeugung gesteckt. Mit höherem Aufwand sind grundsätzlich auch komplexere Lösungen möglich.

Der sich ergebende Aufwand erstreckt sich aber nicht nur auf die Phase der IT-Notfallkonzeptentwicklung, sondern auch auf die periodisch wiederkehrenden Verbesserungen der Konzepte. Wenn zu hohe Ziele gesteckt werden und die dafür erforderlichen Ressourcen nicht in vollem Umfang zur Verfügung stehen, dann wird das Ergebnis schnell in eine unbefriedigende Richtung tendieren. Daraus folgt, dass es entscheidend ist, einen Weg zu finden, eine für das Unternehmen akzeptable IT-Notfallstrategie zu entdecken, deren Niveau auf Dauer gehalten werden kann. Häufig sind oberflächlicher aufgebaute Konzepte effektiver als Konzepte, die in Tausenden von Seiten Papier münden, die bereits nach wenigen Monaten veraltet sind.

Mögliche Strategieoptionen lassen sich als »Minimallösung«, »Kleine Lösung«, »Mittlere Lösung« und »Große Lösung« einordnen. Abhängig vom ermittelten Risiko und den Kosten für abgeleitete Maßnahmen kann man sich jeweils für eine Strategievariante entscheiden. Es sollte eine zusätzliche Richtlinie erstellt werden, die die möglichen Strategien aufzeigt und beschreibt, Maßnahmen nennt und quantifiziert und mit der jeweiligen Risikobetrachtung verknüpft.

7.6 IT-Notfallkonzepte erstellen

Die IT-Notfallkonzepte beinhalten alle Dokumente, die im Rahmen des IT-Notfallmanagements erstellt werden. In ihnen wird schriftlich festgehalten, wie die definierten Notfallstrategien umgesetzt werden sollen. Im Wesentlichen lassen sie sich in zwei Kategorien unterscheiden:



KAPITEL 7 – IT-NOTFALLMANAGEMENT

- die Notfallkonzepte und
- das Notfallhandbuch.

Die Notfallkonzepte beschreiben den Prozess des IT-Notfallmanagements, während die Notfallhandbücher alle zur Durchführung erforderlichen Dokumente zusammenfassen. Das Notfallhandbuch beschreibt alle Stadien vom Auftreten und Quantifizieren eines Notfalls bis hin zur Notfallbewältigung und Nacharbeit. Erfahrungen, die während eines Notfalls gemacht werden und die der Verbesserung dienen können, werden nachträglich sowohl in die Konzeption als auch in die verschiedenen Handbücher eingearbeitet.

Der Regelkreislauf des IT-Notfallmanagements zeigt, auf welche Weise die Aktualisierung der Notfallkonzepte und damit auch des Notfallhandbuchs sichergestellt werden kann. Die Richtlinie zum IT-Notfallmanagement bildet für diesen Kreislauf die Grundlage, da sie sowohl den Auftrag erteilt und die Grundlagen beschreibt als auch Kompetenzen und Verantwortlichkeiten festlegt.

7



Abbildung 7.2: Regelkreis Erstellung der Notfallkonzepte

Die IT-Notfallkonzepte haben die Aufgabe, Antworten auf eine Reihe an Fragen zu finden, die im Rahmen des IT-Notfallmanagements zwangsläufig gestellt werden:



- Planung und Vorbereitung: Welche Vorbereitungen müssen abgeschlossen sein, um im Notfall gewappnet zu sein?
 - Diejenigen Systeme, die vor Ausfall geschützt werden müssen, sind identifiziert.
 - Notfallpläne liegen bereit und werden laufend aktualisiert.
 - Notfallmaßnahmen, die aus den Notfallplänen abgeleitet werden können, sind jederzeit einsatzbereit. Notfallsysteme etc. sind einsatzbereit.
- Technische Vorbereitung: Sind alle benötigten Prozesse und Systeme implementiert?
 - Die Notfallsysteme sind technisch in Ordnung.
 - Die Notfallmaßnahmen sind auf die Produktivsysteme anwendbar.
 - Alarmierungssysteme und Telefonlisten sind aktuell.
- Notfallplanung: Ein Notfall tritt ein, was ist nun konkret zu tun?
 - Wer ist zu informieren, wie sieht das Notfallteam aus und was sind die ersten Schritte?
 - Wo stehen die Notfallpläne und wie ist diesen zu folgen?

7.6.1 Schweregrade

Unterbrechungen des ordentlichen Geschäftsbetriebs können Ursachen von unterschiedlichem Schweregrad haben. Diese wurden bereits im Kapitel »IT Business Continuity Management« aufgeführt.

Hinweis

Auch wenn es verschiedene Schweregrade von Vorfällen gibt, so ähneln sich doch die allgemeinen Vorgehensweisen. Aus diesem Grund wird meistens allgemein von »Notfällen« die Rede sein – auch wenn es sich dabei um schwerwiegender Vorfälle handeln könnte.

1. **(Einfache) Störung:** Als Störung werden alle Ereignisse bezeichnet, die durch die normalen, mit Supportaufgaben befassten Organisationseinheiten behoben werden können. Entstehende Schäden sind als gering einzustufen. Das IT-Notfallmanagement ist üblicherweise für Störungen nicht



KAPITEL 7 – IT-NOTFALLMANAGEMENT

zuständig und sie werden damit auch nicht in den zugehörigen Dokumentationen abgehandelt.

2. **Notfall:** Bei einem Notfall kann die Wiederherstellung des Geschäftsbetriebs nicht innerhalb festgelegter Zeiten stattfinden. In vielen Fällen ist ein Notfall eine eskalierte Störung. Aus diesem Grund ist eine Zusammenarbeit des Krisenstabs mit der Organisationseinheit Support erforderlich. Die Eskalation von Störung zu Notfall ist einer der Trigger, der den Notfallplan oder Teile des Notfallplans aktiviert. Nicht jeder Notfall wird das Zusammenrufen des gesamten Notfallteams zur Folge haben – das ist eher die Ausnahme.

Hinweis

7

Notfälle sind häufig einmalige Vorkommnisse, folgen aber im Allgemeinen Mustern, die einander ähnlich sind. Dadurch können erlernte und in Plänen zusammengefasste Vorgehensweisen zu einer schnellen Lösung führen. So sind Programmierfehler in einer Software zwar jeweils an unterschiedlichen Stellen zu finden und haben auch unterschiedliche Auswirkungen, die einzuleitenden Maßnahmen zur Fehlerbehebung sind aber immer dieselben.

3. **Krise:** Eine Krise ist in den meisten Fällen nicht vorhersagbar, sie beeinflusst einen größeren bis großen Bereich des Unternehmens negativ. Dies kann bis hin zur Gefährdung der Existenz des Unternehmens reichen. Sobald der Krisenfall ausgerufen wird, wird der Notfallplan aktiviert. Im Gegensatz zu einer Störung und häufig auch im Gegensatz zu einem Notfall ist bei einer Krise zumeist zunächst nicht abzusehen, welche Bereiche betroffen sind, und deshalb ist es erforderlich, alle potenziell wichtigen Bereiche mit einzubeziehen. Das ist die Aufgabe des Notfallmanagers.

Hinweis

Nicht jeder Notfall ist eine Krise. Die Entscheidung über die Parameter, die eine Krise zur Krise machen, ist meist fließend und deshalb nicht allgemeingültig zu beantworten. Häufig macht man die Einstufung an den potenziellen monetären Folgekosten fest. Das macht deshalb Sinn, weil



in einer Krise vermutlich weitreichende Entscheidungen zu treffen sind und die Pläne deshalb von vornherein so ausgelegt werden können, dass in diesen Fällen Führungskräfte eingebunden werden, die Entscheidungen mit gewisser Tragweite treffen können.

4. **Katastrophe:** Eine Katastrophe ist eine Krise, die nur zusammen mit externen Organisationen bewältigt werden kann. Für die Bewältigung der Krise existieren keine detaillierten Anweisungen. Im Fokus steht zunächst die Aufgabe, Schaden von Personen abzuwenden und demzufolge sind die Maßnahmen, die in diese Richtung gehen, primär abzuarbeiten.

Hinweis

Zur Katastrophe wird eine Situation dann, wenn die mit Störungen befassten Organisationseinheiten mit ihren Methoden und Maßnahmen nicht mehr ohne Einbezug externer Kräfte in der Lage sind, den Normalzustand wiederherzustellen. Typisch für eine Katastrophe ist deren Einmaligkeit und das daraus resultierende Fehlen von Beschreibungen, wie sie zu bewältigen ist. Typischerweise sind externe Faktoren, wie Erdbeben oder Brände, für das Eintreten verantwortlich.

7

7.6.2 Notfallvorsorge

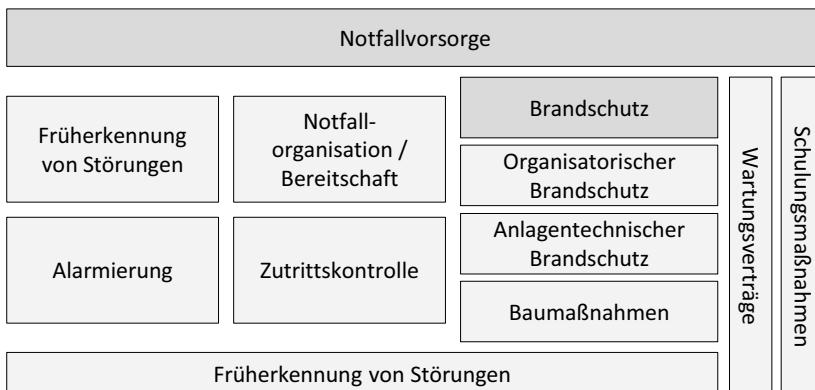
Maßnahmen, die im Rahmen der Notfallvorsorge umgesetzt werden, haben die Aufgabe, die Wahrscheinlichkeit des Eintretens eines Notfalls zu reduzieren. Tritt dennoch ein Notfall ein, so sollen sie zumindest gewährleisten, dass die Situation möglichst schnell und kostengünstig bereinigt wird.

Viele Punkte der Notfallvorsorge werden schon in der IT-Security-Richtlinie verfolgt. Dazu gehören vor allem Aktivitäten in Bezug auf Rechnerräume. Andere Maßnahmen wie Alarmierungsketten, Telefonlisten, Notfallhandbücher oder Schulungsmaßnahmen gehen aus dem allgemeinen IT-Betrieb hervor und finden Eingang in die Notfallhandbücher. So dienen Vorgaben für Rechnerräume zu einem großen Anteil der Notfallvorsorge. Dazu gehören sichere Zugangswege und ein Überwachungs- und Aufzeichnungssystem genauso wie eine unterbrechungsfreie Stromversorgung oder eine redundante



KAPITEL 7 – IT-NOTFALLMANAGEMENT

Infrastruktur zur Klimatisierung. Wieder andere Maßnahmen sind Aufgabe der Rechtsabteilung oder fallen in den Bereich der Organisationseinheiten, die mit dem Abschluss von Versicherungen betraut sind. In Abbildung 7.3 sind die einzelnen Komponenten abgebildet und werden nachfolgend erwähnt. Der Bereich Notfallorganisation wird im nächsten Kapitel vertieft.



7

Abbildung 7.3: Komponenten der Notfallvorsorge

Die Grundlage für die Notfallvorsorge ist die Business-Impact-Analyse. Diese zeigt auf, welcher potenzielle Schaden hinter jedem Systemausfall steckt, und definiert dadurch das maximal in eine Vorsorge zu steckende Budget. Um dies abschließend quantifizieren und auch genehmigen zu können, ist es zudem erforderlich, auch die Aufwände zu kennen, die für die jeweiligen Notfallvorsorgemaßnahmen auftreten werden. Da es häufig nicht effektiv ist, diese explizit für jedes System neu zu kalkulieren, sollten die groben Richtwerte bereits aus den Notfallkonzepten heraus ersichtlich sein.

Ergebnis der Notfallvorsorge sind Pläne, auf denen verzeichnet ist, welche Maßnahme in welcher Reihenfolge von wem zu bearbeiten ist. Neben dem Terminplan sollte noch eine Kostenrechnung mitgeführt werden.

Früherkennung von Störungen

Störungen, die zu Notfällen werden können, treten im Allgemeinen nicht aus heiterem Himmel auf. Verschiedene Indikatoren kündigen sie in vielen Fällen an. Dabei kann es sich um den Verschleiß einer Festplatte handeln oder um Fehlermeldungen, die sich auf einer aktiven Netzwerkkomponente häufen. Die Erfassung und Auswertung dieser Meldungen dient in entscheiden-



dem Maße der Früherkennung von Problemen. Neben der Erfassung der reichen Informationen sind deren Gewichtung und Auswertung entscheidend.

Hinweis

Eine kommende Störung möglichst weit im Voraus zu erkennen, ist in allen Bereichen, in denen zeitkritisch gearbeitet wird, von großem Nutzen. Daher ist es nicht verwunderlich, dass sich im Zusammenhang mit Industrie 4.0 in der Produktion ein eigener Begriff herausgebildet hat. »Predictive Maintenance« beschreibt Techniken, die es erlauben, frühzeitig zu ermitteln, wann eine Produktionsmaschine gewartet werden muss. Etwas Ähnliches gibt es schon länger im Bereich der Drucker. Wird der Toner-Stand zu niedrig, so meldet dies der Drucker selbstständig an den Dienstleister, der den Toner dann auswechseln kann, bevor der Drucker aufhört zu funktionieren.

7

Die Interpretation, was es bedeutet, wenn Festplattenfehler in der Protokolldatei eines Servers auftauchen, lässt sich abschließend oft nur mit der nötigen Erfahrung und der Möglichkeit klären, auf frühere Daten zurückzugreifen. Im Bereich der Hardware ist es heute schon üblich, dass die Hersteller Tools mitliefern, die Ausfälle bereits ankündigen, bevor es bei darauf installierten Betriebssystemen zu Fehlern führt. So können Lesefehler auf Festplatten oder CRC-Fehler bei Speicherzugriffen bereits frühzeitig erfasst und an geeignete Meldesysteme übermittelt werden. Die Früherkennung einer Störung führt bereits zur Alarmierung der entsprechenden Organisationseinheit.

Alarmierung

Der Eintritt einer aktuellen oder prognostiziert bald auftretenden Störung und die Weiterleitung dieser Information an die zuständigen Stellen sind zwei unabhängige Punkte, die oft schwer in Verbindung zu bringen sind. Um eine verlässliche Alarmierungskette aufzubauen zu können, ist es wichtig, im Voraus zu wissen, in welchen Bereichen welche Störungen bearbeitet werden können. Dies kann durch die Beobachtung des Regelbetriebs und durch die Dokumentation in der Vergangenheit vorgekommener Notfälle unterstützt werden. Dazu müssen wichtige Systeme in eine automatisierte Alarmierung integriert werden. Dies kann technisch, durch entsprechende Softwarepro-



dukte oder aber manuell durchgeführt werden. Wichtigen Input liefert dabei auch die Business-Impact-Analyse. Durch sie wird definiert, welche Systeme vorrangig in eine Überwachung genommen werden müssen. Die automatisierte Alarmierung wird im Allgemeinen durch Monitoring-Systeme ausgelöst.

Brandschutz

Hinweis

Der Brandschutz steht stellvertretend für alle baulichen Vorsorgemaßnahmen. So muss, abhängig vom Standort und der Wichtigkeit der IT-Systeme, genauso gegen Wasser, Blitzschlag, Erdbeben, Erdrutsche und andere naturbedingte Notfälle vorgesorgt werden.

7

Brandschutz im Sinne des Business Continuity Managements beinhaltet sowohl Maßnahmen, die im Vorfeld umgesetzt werden, um das Risiko eines Brandes zu minimieren, als auch Richtlinien, wie die Brandbekämpfung im Notfall durchzuführen ist.

Organisatorischer Brandschutz

Bricht ein Brand aus, so muss die Alarmierungskette vom Brandmelder bis zur Nutzung von Telefonlisten und darüber hinaus lückenlos vorhanden sein. Im Normalfall sind Sensoren installiert, die, falls sie ausgelöst werden, automatisch externe Rettungskräfte und internes Personal benachrichtigen. Tritt der Notfall nachts oder am Wochenende ein, so kann es erforderlich werden, das Notfallteam zu benachrichtigen, damit dieses in Zusammenarbeit mit der Feuerwehr Rettungsmaßnahmen anhand von Prioritätslisten durchführt. Steht ein Rechenzentrum in Brand, so ist es z.B. zweckmäßig, zunächst diejenigen IT-Systeme zu retten, die kritisch für das Unternehmen sind.

Baumaßnahmen

Bei der Konzeption und beim Bau eines Rechenzentrums oder anderer Räumlichkeiten, in denen wichtige IT-Systeme oder Datenträger untergebracht sind, müssen vielfältige bauliche Besonderheiten beachtet werden. Diese erstrecken sich von der Örtlichkeit an sich über verwendete Baustoffe



bis hin zu Brandwänden, die Brandabschnitte voneinander trennen. Die Regel, dass Daten und Backup-Systeme durch Brandabschnitte voneinander getrennt werden müssen, findet an dieser Stelle Anwendung und muss durch entsprechende Maßnahmen umgesetzt werden. Eine weitere Regel ist die, dass Ausweichrechenzentren in einem weiteren Gebäude zu installieren sind, das mindestens einen Abstand zum ersten Gebäude einhält, der der Höhe des primären Gebäudes entspricht. Zudem sind diese Rechenzentren in verschiedenen Etagen einzurichten. Auf diese Art kann bei einer Überflutung nur ein Rechenzentrum direkt betroffen sein.

Rechenzentren und IT-Systeme sind niemals vollständig autark. Sie sind durch stromführende Leitungen und Netzwerkabel mit weiteren Systemen verbunden, die oftmals in weniger stark gesicherten Räumen untergebracht sind. Da sich Feuer entlang dieser Kabel in Form von Kabelbränden verbreiten kann, sind zudem entsprechende Abschottungsmaßnahmen durchzuführen.

Anlagentechnischer Brandschutz

Zur Brandbekämpfung stehen vielfältige Möglichkeiten zur Verfügung. Diese Möglichkeiten werden unter dem Begriff »Anlagentechnischer Brandschutz« geführt. Zu ihnen gehören alle Arten von Feuerlöschanlagen. Abhängig von der Art des Brandherdes sind entsprechende Löschanlagen zu bevorraten. Daneben können Abläufe implementiert werden, die streckenweise automatisiert ablaufen können. Zu den automatisiert ablaufenden Maßnahmen gehört z.B. die Flutung von Räumen mit Halon-Gas.

Zutrittskontrolle

Ein durch Sabotage, den Elektriker oder das viel zitierte Reinigungspersonal ausgelöster Notfall kann durch eine geregelte Zutrittskontrolle weitgehend vermieden werden. Dabei ist es nicht nur wichtig, möglichst wenigen Personen Zutritt zu gewähren, sondern, falls Arbeiten z.B. in einem Computerraum erforderlich werden, diesen Personen geschultes IT-Personal zur Seite zu stellen, um die durchgeführten Tätigkeiten zu überwachen.

Schulungsmaßnahmen

Viele Störungen und Notfälle sind auf das Fehlverhalten interner oder externer Mitarbeiter zurückzuführen. In den allermeisten Fällen wird dies nicht absichtlich geschehen sein. Ob es sich um die Falschverwendung geheimer



Informationen handelt oder um die Fehlbedienung eines Systems, ist dabei zweitrangig. In beiden Fällen wäre der Fehler oft vermeidbar gewesen, wenn der Mitarbeiter im Umgang mit Informationen und mit IT-Systemen ausreichend geschult und sensibilisiert worden wäre.

Das Schulen von Mitarbeitern und die Steigerung der Awareness ist eine zentrale Aufgabe der IT-Security. Den richtigen Umgang mit IT-Systemen zu erlernen und damit einen Teil zur Notfallvorsorge zu treffen, ist eine wichtige Ergänzung zu den üblichen Schulungsmaßnahmen.

Wartungsverträge

7

Verträge mit Lieferanten von Hardware und Software werden weit im Vorfeld eines eventuellen Notfalls getroffen. Im Fall der Fälle ist es wichtig, die entsprechenden Bedingungen und Telefonnummern der Lieferanten im Zugriff zu haben. Dabei kann es um den schnellen Austausch von Hardwarekomponenten oder aber um die Behebung eines gravierenden Softwareproblems gehen. In beiden Fällen hängt die Fix-Time von den vertraglichen Bestimmungen ab. Aus diesem Grund sollten die Vereinbarungen auf den Service Level Agreements basieren, die im Rahmen der Business-Impact-Analyse festgelegt wurden.

Verlagerung des Risikos auf Dritte

Einen Notfall zu versichern, ist keine Vorsorge im eigentlichen Sinne. Vielmehr wird die nachträgliche Begleichung von Schäden auf einen Versicherer abgewälzt. Um einen Schaden nach einem Notfall durch einen Versicherer abwickeln zu lassen, muss man nachweisen können, dass der Schaden durch die Versicherung abgedeckt war. Diese Tatsache bedingt ein Minimum an Dokumentation und Nachvollziehbarkeit. Zusätzlich dazu wird ein Versicherer gewisse Mindeststandards an die Notfallvorsorge einfordern. Die Einbindung des Versicherers in den Krisenmanagement-Prozess ist in vielen Cybercrime-Versicherungsverträgen fest vorgeschrieben. Dadurch will der Versicherer vermeiden, dass ein Notfall durch ein mangelhaftes Vorgehen höhere Kosten verursacht als unbedingt erforderlich. Für das Unternehmen hat dies wiederum den Vorteil, dass geschultes, externes Personal bereitsteht, die eigenen Notfallteams zu unterstützen. Funktioniert diese Zusammenarbeit gut, handelt es sich um eine klassische Win-win-Situation.



7.7 Notfallorganisation

Tritt ein Notfall ein, so ist schnelles und effektives Handeln gefordert. Missverständnisse, Doppelarbeit oder unklare Kompetenzen verhindern die Umsetzung dieses Grundsatzes und müssen deshalb schon im Vorfeld weitestgehend ausgeräumt werden. Aus diesem Grund ist die von der Unternehmensleitung abgesegnete Struktur der Notfallorganisation ein Basiselement des IT-Notfallmanagements.

7.7.1 Organisationsstruktur

Tritt ein Notfall ein, so müssen alle Personen zusammengerufen werden, die zur Notfallbewältigung beitragen können. Der dafür benötigte Personenkreis entspricht im Normalfall nicht vollständig demjenigen, der für den Normalbetrieb zuständig ist. Das hat viele Gründe. Zum einen ist es erforderlich, im Notfall eine zentrale, abteilungsübergreifende Anlaufstelle zu haben, in der die endgültigen Entscheidungen getroffen werden. Zum anderen können die Anforderungen an Mitarbeiter in einem Notfall stark von denen im alltäglichen Arbeitsleben abweichen. Da Notfälle auch außerhalb der normalen Arbeitszeiten auftreten können, sind zudem Themen wie Bereitschaftsregelungen und der Einsatz externer Mitarbeiter bzw. externem Support zu regeln und in die Planung der Notfallorganisation zu integrieren. Dadurch ergeben sich in Notfällen Gruppen, die es oft nicht gewohnt sind, miteinander zu arbeiten. Hinzu kommt, dass Verantwortlichkeiten in Notfällen oft nicht den üblichen Führungsstrukturen entsprechen. Alle diese Punkte verlangen nach einer stringenten und klar definierten Notfallorganisation.

Mindestens drei Führungsebenen sind für die Bereiche Notfallvorsorge und Notfallbewältigung einzuplanen:

1. **Strategische Ebene:** Die Managementebene, in der in letzter Konsequenz die Entscheidungen bezüglich des IT-Notfallmanagements getroffen werden. Häufig handelt es sich dabei um die Verantwortlichen für alle Bereiche des Business Continuity Managements.
2. **Taktische Ebene:** Die Personen, die bei einem Notfall die Leitung übernehmen und in der Notfallvorsorge alle Aktivitäten bündeln und koordinieren. In der Notfallbewältigung wird diese Ebene auch »Krisenstab« genannt. In



der Notfallvorsorge handelt es sich um den »Notfallbeauftragten« oder auch »Notfallkoordinator«.

3. **Operative Ebene:** Die Notfallteams der operativen Ebene berichten an die taktische Ebene und sind für die Umsetzung der Maßnahmen aus dem Notfallplan zuständig.

Hinweis

Grundsätzlich gilt, dass viele Rollen in der Notfallorganisation nach außen vergeben werden können. Das ist nicht nur für die operative Ebene üblich, viele Unternehmen geben auch die strategische Ausrichtung des IT-Notfallmanagements in die Hände externer Berater. Im Falle eines versicherten Cyber-Angriffs kann es sich um ein Team handeln, das vom Versicherer bereitgestellt wird.

7

Je größer ein Unternehmen ist und die Anzahl der Standorte wächst, desto wichtiger wird die Frage nach einer zentralen Koordination des IT-Notfallmanagement-Prozesses. Da diese Aufgabe einiges an Fachwissen erfordert, wird sie üblicherweise nicht von der Unternehmensleitung bzw. der Managementebene wahrgenommen, die für IT-Notfallmanagement zuständig ist, und liegt damit irgendwo zwischen der strategischen und der taktischen Ebene.

7.7.2 Kompetenzen und Zuständigkeiten

Der Übergang vom Normal- zum Notfallbetrieb bringt automatisch auch eine Verschiebung von Rollen und Zuständigkeiten mit sich. Sobald die Notfallorganisation greift und die dort definierten Mitarbeiter die Notfallbewältigung starten, beginnt auch eine Verschiebung von Kompetenzen. Dies kann schnell zu Konflikten führen, wenn die Bedürfnisse des normalen Betriebs mit denen der Krisenteams kollidieren. So kann die Reparatur eines Systems dazu führen, dass temporär ein zweites, bislang funktionsfähiges System kurzfristig deaktiviert werden muss. Die Schnittstellen und die dann jeweils geltenden Kompetenzen müssen bereits in der Notfallvorsorge definiert werden. Gibt es keine Überschneidungen, so fällt die Trennung leichter: Die für den Regelbetrieb verantwortlichen Stellen betreiben weiterhin alle nicht vom



Notfall betroffenen Systeme und die Notfallteams jene Systeme, die Teil des Notfalls sind.

Der Krisenstab übernimmt die Leitung des Notfallteams und hat in allen relevanten Fragen die Verantwortung. Dazu ist die fachliche Weisungsbefugnis über die Mitglieder des Notfallteams erforderlich. Wenn der Krisenstab mit Führungskräften besetzt ist und je weitgehender das Notfallteam der üblichen Teamzusammensetzung entspricht, desto einfacher ist dies umzusetzen.

7.7.3 Notfallhandbuch

Bei einem Notfall ist es wichtig, schnell und unkompliziert alle relevanten Informationen für dessen Bewältigung zur Hand zu haben. Dafür ist es zum einen wichtig, dass ein Notfallhandbuch griffbereit ist, und zum Zweiten, dass der Aufbau so gestaltet ist, dass ein längeres Durchstöbern unnötig ist. Beherzigt man diese beiden Vorgaben, dann erscheint es sinnvoll, neben einer rein IT-gestützten elektronischen Version auch einen physischen Ordner zur Hand zu haben. So ist es im Normalbetrieb angenehm, durch ein Web-basiertes System zu browsen. Durch die dort mögliche Verknüpfung von Themen springt man schnell und logisch geordnet durch verwandte Themen. Eine Volltextsuche hilft zudem, die relevanten Inhalte zu sortieren und auffindbar zu machen. Im Notfall kann dies wieder ganz anders aussehen. Sind die Räumlichkeiten, in denen der Notfall bearbeitet wird, nicht mit den entsprechenden Systemen zur Anzeige des Notfallhandbuchs ausgestattet, so ist auch kein Zugriff möglich. Im schlimmsten Fall sind auch die Systeme vom Notfall betroffen, die zur Anzeige des Notfallhandbuchs erforderlich sind. Dies sind Gründe, warum in vielen Rechenzentren Ordner mit Notfallhandbüchern aus Papier stehen. Dies ist der Fall, obwohl Handbücher aus Papier wieder gänzlich anderen Problemen ausgesetzt sind. Angenommen, es existiert ein Dutzend Ordner, die verteilt an verschiedenen Standorten abgelegt sind, dann ist der Prozess der Aktualisierung bereits so umfangreich, dass dafür ein eigener Wartungsprozess eingerichtet werden muss.

Die Gliederung des Notfallhandbuchs passt sich unweigerlich dem technischen Unterbau an. Liegt das Handbuch in Papierform vor, so werden die Ansprüche an logischen Aufbau höher sein, als wenn es in elektronischer Form vorliegt, da dort Möglichkeiten zum Durchsuchen und Verlinken vorhanden sind.



Auszug aus dem Notfallhandbuch der Firma XYZ

1. Einleitung
 - a. Überblick Version
 - b. Überblick referenzierter Dokumente
 - c. Überblick Wartungsverträge, SLAs und Lieferanten
2. Verzeichnis Ansprechpartner
 - a. Ansprechpartner in Notfällen
 - b. Verzeichnis öffentliche Stellen
 - c. Internes Telefonverzeichnis
 - d. Interne Bereitschaft
3. Sofortmaßnahmen in Notfällen
 - a. Maßnahmen im Fall von Feuer
 - b. Maßnahmen im Fall von Wassereinbruch
 - c. Maßnahmen im Fall von IT-Systemausfall
4. IT-Infrastrukturübersicht
 - a. Netzwerktopologie
 - b. Speichersysteme
 - c. Backup / Restore
 - d. Serverlandschaft
5. Notfallbewältigung
 - a. Rollen, Zuständigkeiten und Kompetenzen
 - b. Alarmierungsweg
 - c. Notfallbewältigung
 - I. Erste Schritte
 - II. Besprechungsraum
 - III. Beurteilung der Lage
 - IV. Risikobeurteilung
 - d. Disaster Recovery
 - I. Wiederherstellungspläne
 - II. Wiederanlaufpläne
 - III. DR Computerraum
 - IV. DR Serverlandschaft
 - V. DR Netzwerk
 - VI. DR Telekommunikation
 - e. Überblick Services und geplanter Notbetrieb
 - f. Dokumentation Notfallbewältigung
6. Anhang A
 - a. Übersicht Geschäftsprozesse und Klassifizierung
 - b. Übersicht Verantwortlichkeiten für Geschäftsprozesse

Abbildung 7.4: Beispielhaftes Notfallhandbuch

Grundsätzlich gibt es innerhalb eines Notfallhandbuchs Bereiche, die häufigen Änderungen unterworfen sind, und andere, die statischer sind. Um Anpassungen schneller und direkter durchführen zu können, ist es sinnvoll, die häufiger von Änderungen betroffenen Bereiche von den statischeren abzutrennen. Durch diese Modularisierung ist es zudem möglich, einzelne Bereiche des Handbuchs in verschiedene Verantwortlichkeitsbereiche zu legen. So können z.B. Telefonlisten durch Personen aktualisiert werden, die mit der technischen Seite eines Notfalls üblicherweise nicht betreut sind.

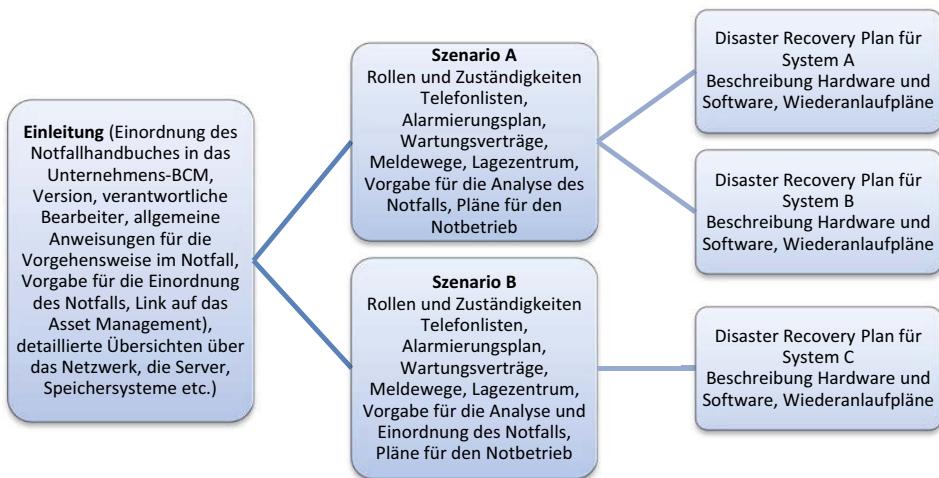


Abbildung 7.5: Schritte zum Aufbau eines Notfallhandbuchs

7

Für den Aufbau des Notfallhandbuchs sind verschiedene Gliederungen denkbar, die sich stark an der Organisationsgröße, an der Art des Notfalls und dem Umfang der einzuleitenden Maßnahmen orientieren. Oberste Prämisse ist, dass im Notfall alle erforderlichen Informationen direkt zugänglich sein müssen. Die Notfallbewältigung folgt logischen Schritten: von der Alarmierung zur Analyse des Notfalls, der Bildung des Teams bis hin zur technischen Abarbeitung von Maßnahmen. Diese Schritte können eine grobe Gliederung darstellen.

Eine andere Sichtweise ist dann zu wählen, wenn verschiedene Fachbereiche in die Notfallbewältigung mit eingebunden sind. In diesem Fall orientiert sich die Gliederung oft an den Rollen und Zuständigkeiten der einzelnen Mitarbeiter im Notfallteam. Auch eine Trennung von organisatorischen Informationen wie Telefonlisten, Wartungsverträgen und Festlegungen für die Alarmierung und technische Wiederanlaufpläne wird häufig angewendet.

7.8 Notfallbewältigung

Nicht für jedes Szenario muss und kann ein Vorgehensplan entworfen werden. Auf der anderen Seite können einige Vorgehenspläne bei unterschiedlich gelagerten Notfällen angewandt werden. Manchmal ist auch eine Mischung aus Vorgehensplänen hilfreich.



KAPITEL 7 – IT-NOTFALLMANAGEMENT

Davon ausgehend, dass alle Notfallpläne vorliegen, das Krisenteam bereits eingetroffen ist und das Handbuch mit den Vorgehensplänen zur Hand nimmt, werden ganz automatisch vordefinierte Schritte eingeleitet. Beim Eintritt eines Notfalls werden zunächst alle Maßnahmen ergriffen, um Gefahr für Leib und Leben von Personen abzuwenden. Handelt es sich um Feuer oder einen Wassereinbruch, so ist sicherzustellen, dass Feuerwehr und andere Rettungskräfte gerufen werden. Sind entsprechende Alarmierungseinrichtungen installiert, dann wird dies zum Teil automatisch geschehen. Falls nicht oder für den Fall, dass alle Meldungen zunächst in einer eigenen Meldestelle einlaufen, ist dafür Sorge zu tragen, dass auf diese Meldungen angemessen und schnell reagiert wird. Dafür sind Handbücher und Vorgehensbeschreibungen zu hinterlegen.

7

Sind die ersten, offensichtlich erforderlichen Maßnahmen getätigt, dann ist die Prämisse für alle weiteren Arbeiten zunächst einmal diese: Ruhe bewahren! Schnelles und unkoordiniertes Eingreifen aus einer Stimmung der Aufgeregtheit heraus kann schnell weiteren Schaden anrichten, der umso schwerer wieder zu beseitigen ist, da er häufig Systeme betrifft, die bislang außen vor waren und jedes zusätzliche System die allgemeine Komplexität des Problems erhöht. In manchen Handbüchern ist deshalb der Satz zu lesen: »Nach Alarmierung der zuständigen öffentlichen Stellen und der Alarmierung des Krisen- und Notfallteams muss auf das Eintreffen der Koordinatoren für die Krise gewartet werden.«

Zunächst einmal ist es verwunderlich zu lesen, dass bei einem Notfall nichts getan werden soll, wenn es nicht dem Löschen eines Feuers oder der Bergung von Verwundeten dient. Auf den zweiten Blick ist dies aber durchaus sinnvoll. Erst muss sich der Verantwortliche einen Überblick verschaffen, bevor Maßnahmen eingeleitet werden. Im Zuge der steigenden Komplexität der IT-Landschaften und hinsichtlich hochgradig voneinander abhängiger IT-Systeme ist es wichtig, das Richtige zum richtigen Zeitpunkt zu tun. Ein weiterer wichtiger Punkt ist der, dass Parallelarbeiten an Systemen nur dann stattfinden sollten, wenn sichergestellt ist, dass diese nicht voneinander abhängig sind. Im einfachsten Beispiel ist die Wiederherstellung einer Datenbank aus einem Backup nicht erfolgreich, wenn gleichzeitig der Core-Switch neu gestartet wird, an dem die Backup/Restore-Einheiten angeschlossen sind. Die Aufgabe des Verantwortlichen ist es, das Gelingen der beiden Maßnahmen durch zielgerichtete Koordination sicherzustellen. Die Aufgabe seines Krisenteams ist es, ihn mit den richtigen Informationen zu versorgen, damit er die richtigen Entscheidungen treffen kann.



In überschaubaren Notfällen ist dies oft formlos möglich. In ausgeweiteten, eventuell mehrere Rechenzentren betreffenden Notfällen ist dies nicht mehr ganz so einfach. In diesen Fällen sollte die Möglichkeit geschaffen werden, dass sich der Verantwortliche regelmäßig in geeigneten Räumlichkeiten mit seinen Krisenteams trifft. Diese Art von planvollem und stringentem Vorgehen senkt den Stress und vermeidet Hektik, die sich schnell auf die Arbeitsqualität auswirken kann. Ruhe zu bewahren und diese Ruhe bis in die Notfallteams auszustrahlen, ist eine weitere wichtige Aufgabe der Verantwortlichen.

Hinweis

Die Notfallbewältigungsmaßnahmen beinhalten, neben den formalen Rahmenbedingungen wie die Treffen der Notfallteams, vor allem auch die Notfallwiederherstellung (engl. Disaster Recovery) der betroffenen IT-Systeme. Diesem Vorgang wird ein großer Teil des Notfallhandbuchs gewidmet, dessen Aktualität von großer Wichtigkeit ist. Teile dieses Plans beinhalten den Ersatz beschädigter Hardware oder die Datenwiederherstellung aus dem Backup.

7

Durch eine geeignete Positionierung des Verantwortlichen und des Krisenteams in der Befehlshierarchie ist es vor Ort möglich, wichtige Entscheidungen zu treffen. Viele davon werden unvorhersehbar und neu sein. Trotz der vielen und zeitlich kritischen Fragen, die entschieden werden müssen, ist es erforderlich, dass jede einzelne Entscheidung auf einer ad hoc durchgeföhrten Risikobetrachtung basiert. Was passiert, wenn ich entscheide, ein System vom Netz zu nehmen? Welches Risiko entsteht für den Betrieb, wenn ich Kernkomponenten des Netzwerks austausche? Der Überblick über die gesamte IT und ein Gefühl für Auswirkungen im Betrieb bzw. auf die Notfallbewältigung in anderen Bereichen sind unerlässlich für eine möglichst schnelle und sichere Abwicklung des Notfalls.

Es gibt Entscheidungen während einer Notfallbewältigung, deren Tragweite nicht vorhergesehen werden kann und für die es Alternativszenarien geben sollte. Eine solche könnte z.B. sein, dass der Verantwortliche entscheidet, eine Datenwiederherstellung mit Datenrettungstools von beschädigten Speicherplatten zu versuchen, da eine Wiederherstellung nicht alle aktuellen Daten enthalten würde. Die Entscheidung, dass so vorgegangen werden soll, ist die



KAPITEL 7 – IT-NOTFALLMANAGEMENT

eine; wann der Versuch aufgegeben werden muss, um auf die Wiederherstellung als zweitbeste Lösung zurückzugreifen, ist eine weitere. Für eine solche Entscheidung sind Service Level Agreements genauso einzukalkulieren wie erforderliche Zeiten und die allgemeine Abschätzung der Lage.

Aus der Notfallvorsorge, aus den Notfallübungen und aus dem Notfallhandbuch heraus können viele Entscheidungskriterien für das Vorgehen in einem spezifischen Notfall abgeleitet werden. So kann die Klassifizierung von Geschäftsprozessen und anhängiger IT-Systeme für die Risikobetrachtung im Notfall herangezogen werden. Ablaufpläne und IT-Infrastrukturübersichten sind wichtig für das große Bild. Pläne für den Notbetrieb sind essenziell, um auch komplexe Systeme in geeigneter Weise in alternative Szenarien überführen zu können. Wenn man z.B. bedenkt, welche Arbeiten erforderlich sind, wenn ein Alternativrechenzentrum in Betrieb genommen oder ein Cluster-System umgezogen werden muss, dann ist einzusehen, dass dafür detaillierte Handlungsbeschreibungen erforderlich sind. Diese Handlungsanweisungen können wie folgt strukturiert werden.

Störung	Erforderliche Gerätschaften/Mitarbeiter/Dokumentationen	Handlungsanweisung
Klimagerät im Rechenzentrum ist ausgefallen	Ventilator, Wartungspersonal für Klimageräte, Abschaltliste unkritischer Systeme	Techniker und zuständige IT-Mitarbeiter rufen, Ventilatoren aufstellen, für stetigen Luftstrom sorgen, niedrig klassifizierte Gerätschaften abschalten
Hereinkommende (incoming) E-Mail funktioniert nicht	Übersichtsplan Mailkette	Zuständige IT-Mitarbeiter rufen, Prüfkatalog Mailkette abarbeiten: Mailgateway-Protokoll prüfen, Antispam- und Antiviren-Server überprüfen, MX-Eintrag beim Provider prüfen, Mailserver-Log auswerten, Netzwerk prüfen
Ausfall Produktionsystem mit unbekannter Ursache	Server- und Netzwerkdokumentation	Zuständige Mitarbeiter rufen, Netzwerk prüfen, SAN prüfen, Server prüfen, Anwendungen prüfen

Tabelle 7.1: Rudimentäre Tabelle mit Handlungsanweisungen im Fehlerfall



Für einfache Ausfälle z.B. bei Defekten an Servern oder Klimaanlagen oder bei Versagen von bestimmten Prozessen ist es häufig möglich, bereits im Vorfeld Handlungspläne zu entwerfen. Dies ist vor allem dann wichtig, wenn nicht immer sichergestellt werden kann, dass die entsprechenden Experten bei einem Notfall vor Ort kommen bzw. von einem Fernarbeitsplatz aus eingreifen können. Ein solcher Ablaufplan kann beliebig detailliert gestaffelt aufgebaut sein. Zu große inhaltliche Tiefe ist oft schwer zu warten und aktuell zu halten. Zu geringe Tiefe und zu wenig detailliert ausgeführte Arbeitsanweisungen wiederum führen zu Nachfragen, die eventuell nicht bedient werden können. Für die eben erwähnten einfachen Fälle sind oft übersichtliche Tabellen im Einsatz. Ein grobes Beispiel können Sie in Tabelle 7.1 sehen. Die dort aufgeführten Punkte in der Spalte »Handlungsanweisung« können dabei Links auf weiterführende Handbücher enthalten.

7.9 Notfallübungen

Notfallübungen sind ein wesentlicher Teil der Notfallvorsorge. In ihnen werden alle Phasen des IT-Notfallmanagements auf Tauglichkeit überprüft. Nur dadurch ist es möglich, Fehler in der Prozesskette zu identifizieren und zu beseitigen. Notfallübungen können in zwei unterschiedlichen Formen durchgeführt werden: zum einen in Form von geplanten und zum anderen in Form von unangekündigten Notfallübungen. Geplante Übungen werden häufig in genau abgegrenzten Bereichen angesetzt, um die aufgesetzten Prozesse zu überprüfen. Sie stellen damit einen wichtigen Teil der Auditierung dar. Aufgrund der Tatsache, dass Personal explizit eingeplant wird und der Stresslevel eher gering ist, lassen geplante Übungen nur bedingt Rückschlüsse zu, ob das IT-Notfallmanagement im Ganzen funktioniert. Unangekündigte Notfallübungen, im Idealfall von Bereichen angestoßen, die nicht in die Behebung involviert sind, finden eher in einem Umfeld statt, das nahe an echten Notfällen agiert. Vor allem die Interaktion zwischen den verschiedenen Verantwortlichen kann dabei erfolgreich getestet werden.

Die Ergebnisse einer Notfallübung sollen am Ende über die Bereiche Notfallplanung, Umsetzung von Notfallplänen, Notfallorganisation und Effizienz Rückschlüsse zulassen. Da der Umgang mit Notfällen auf Konzepten beruht, die zum Teil weit im Vorfeld erstellt wurden, stehen dabei deren Aktualität und Korrektheit auf dem Prüfstand. Dazu kommt die Kluft zwischen theoretischen Vorgehensbeschreibungen und der Wirklichkeit, deren Überbrü-



ckung einen entscheidenden Teil der Notfallübung darstellt. Dabei stellt sich die Frage, ob die beschriebenen Prozesse in der geplanten Form und Effizienz durchführbar sind, ob nicht Bindeglieder fehlen oder ob es nicht einen besseren Weg gibt, die formulierten Ziele zu erreichen. Daraus kann man erkennen, dass das Ergebnis einer Notfallübung kein schlichtes »hat funktioniert« oder »hat nicht funktioniert« ist, sondern dass alle Prozessstufen einzeln bewertet und gegebenenfalls angepasst werden sollten.

Notfallübungen sollten regelmäßig wiederholt werden, um dem technischen Fortschritt und geänderten Zuständigkeiten gerecht zu werden. Parallel dazu muss das Notfallkonzept auch abseits von Notfallübungen ständig weiterentwickelt werden.

7

7.10 Überprüfung des IT-Notfallmanagements

Je heterogener ein IT-Umfeld ist, desto umfangreichere und vielfältigere Maßnahmen zum IT-Notfallmanagement werden installiert sein. Eine Überprüfung, ob die verschiedenen Bereiche ausreichend geschützt sind, kann z.B. über »Scorecards«, wörtlich übersetzt »Bewertungskarten« erfolgen. Dabei werden die entscheidenden Kriterien abgefragt, um Vollständigkeit zu erreichen. Auf dieser Basis können die Notfallprozesse hinterfragt und auditiert werden.

Laufende Nummer	Kriterium
1.	Ein IT-Notfallmanagement, als Bestandteil des Business-Continuity-Plans, ist vorhanden.
2.	Das IT-Notfallmanagement wurde durch entsprechende Simulationen verschiedener Szenarien getestet.
3.	Die Ergebnisse aus dem Test des IT-Notfallmanagements lassen den Schluss zu, dass die dort definierten Prozesse stimmig sind und auftretende Notfälle abdecken.
4.	Notfallübungen werden regelmäßig (mindestens einmal im Jahr) durchgeführt. Die daraus erzielten Ergebnisse fließen in die Verbesserung der Notfallprozesse und -handbücher ein.
5.	Die Notfallteams sind benannt. Jedes Mitglied des Notfallteams weiß um seine Rolle und ist darin geschult.



Laufende Nummer	Kriterium
6.	Ein Prozess existiert, der für die Aktualität und Verfügbarkeit der jeweils neuesten Version aller Handbücher Sorge trägt.
7.	Die Unternehmensführung wird über den aktuellen Stand des Business-Continuity-Plans informiert und trägt die Maßnahmen, die daraus abgeleitet werden.
8.	Die für die Bewältigung eines Notfalls erforderliche IT-Infrastruktur steht bereit. Deren Funktionsfähigkeit ist sichergestellt.
9.	Ein Meldewesen ist implementiert. Dieses stellt sicher, dass Notfälle innerhalb der definierten Zeitspannen gemeldet werden. Der Meldevorgang stellt sicher, dass die Behebung des Notfalls im Laufe der akzeptablen Zeitspanne erfolgt.

7.11 Monitoring im Rahmen des IT Business Continuity Managements

Eine Teilaufgabe des System-Monitorings von IT-Systemen oder Applikationen liegt in der Erkennung von Störungen und Notfällen und in der entsprechenden Alarmierung der zuständigen Stellen. Ausfälle von ganzen IT-Systemen, die für den Betrieb wichtiger Geschäftsprozesse erforderlich sind, können direkt einen Alarm auslösen und per E-Mail oder SMS den zuständigen Mitarbeiter informieren. In diesem Fall wird er neben der reinen Meldung auch sofort auf das fehlerhafte System hingewiesen, was die Ursachenforschung maßgeblich abkürzt.

Der Zweck einer Echtzeitüberwachung von IT-Systemen ist, Unregelmäßigkeiten automatisiert zu entdecken und zu melden. Die Meldung kann dabei auf einem Überwachungsmonitor auflaufen oder aber direkt die Alarmierung auslösen. Die Überwachung erfolgt in diesem Fall z.B. durch ein Monitoring-System, das andere Systeme auf Port- oder Dienstebene überwacht. Ein Beispiel ist die Überwachung durch Nutzung des TCP/IP-Protokolls ICMP. In diesem Fall werden ICMP-Pakete (ping) an ein Zielsystem geschickt und darauf gewartet, ob eine Antwort erfolgt. Erfolgt eine Antwort, ist das Zielsystem über das Netzwerk erreichbar. Die Dauer der Paketübermittlung sagt zudem etwas über die Latenz der Leitung aus. Verfolgt man noch den Weg der Pakete (*traceroute*), dann kann im Problemfall ermittelt werden, an welcher Stelle die



KAPITEL 7 – IT-NOTFALLMANAGEMENT

Kommunikation unterbrochen ist. Alle diese Parameter sind in einem Produktivsystem wichtige Hinweise auf Probleme. Tritt eine Fehlfunktion ein, so helfen sie dabei, die Art des Problems und den Schweregrad einzuschätzen, um ein effektives und angemessenes IT-Notfallmanagement in Gang zu setzen. Das Monitoring ist damit ein wichtiger Auslöser für ein IT-Notfallmanagement.

Eine weitere Art des Monitorings stellt die Auswertung von Protokolldateien dar. In diesem Fall werden von Systemen oder Software generierte Daten ausgelesen und analysiert. Diese Art des Monitorings kann sowohl im Nachhinein zur Fehleranalyse oder zum Aufdecken von Sicherheitsproblemen dienen als auch genutzt werden, um in Echtzeit Fehler zu erfassen und wiederum ein IT-Notfallmanagement zu starten.

7

7.12 Checklisten IT-Notfallmanagement

Die folgenden Checklisten zum IT-Notfallmanagement decken grundlegende Fragen ab, die sich der Verantwortliche für diese Thematik stellen sollte. Abhängig von der individuellen Situation und technischen Umgebung sollten die Checklisten so weit erweitert werden, dass alle relevanten Bereiche abgedeckt sind.

7.12.1 Checkliste Business-Impact-Analyse

BIA01	Wurden die kritischen Geschäftsprozesse erfasst und die IT-Systeme identifiziert, die diese unterstützen?
BIA02	Wurden im Rahmen eines IT-Risikomanagements die Risiken des Ausfalls von Prozessen und IT-Systemen betrachtet?
BIA03	Wurde eine Auflistung der Bedrohungen und der möglichen Schäden für die erfassten IT-Systeme erstellt?
BIA04	Wurden die gelisteten IT-Systeme nach einem Klassifizierungsschema priorisiert? Die Klassifizierung sollte für die Schutzziele Vertraulichkeit, Verfügbarkeit, Belastbarkeit und Integrität durchgeführt werden.
BIA05	Sind für die gelisteten IT-Systeme (bzw. für die darüber liegenden Prozesse) Service Level Agreements definiert worden? Sind maximal tolerierbare Ausfallzeiten festgelegt worden?

Tabelle 7.2: Checkliste Business-Impact-Analyse



BIA06	Wurde ein Prozess definiert, der die laufende Aktualisierung der Klassifizierung und der Risikoeinstufungen sicherstellt?
BIA07	Wurde ein Prozess installiert, der die Dokumentation jeder Änderung sicherstellt, die die Dokumente des IT-Notfallmanagements betrifft?
BIA08	Wurden die Ergebnisse der Business-Impact-Analyse mit der Unternehmensleitung abgestimmt?
BIA09	Passen die Bewertungsregeln der Business-Impact-Analyse (Klassifizierung und Einordnung aufgrund des IT-Risikomanagements) mit denen des Unternehmensrisikomanagements zusammen?
BIA10	Wurden bei der Betrachtung von Prozessen und IT-Systemen auch die kritischen Applikationen betrachtet?
BIA11	Wurden die Datenströme zwischen Anwendungen betrachtet? Sind Abhängigkeiten zwischen IT-Systemen und zwischen Teilprozessen ausreichend berücksichtigt?
BIA12	Wurde eine Liste kritischer Cloud-Anwendungen erstellt und ist deren Verfügbarkeit gewährleistet?

Tabelle 7.2: Checkliste Business-Impact-Analyse (Forts.)

7.12.2 Checkliste Notfallorganisation

ORG01	Ist die Notfallorganisation definiert und beschrieben? Sind alle Mitglieder der Notfallteams definiert?
ORG02	Sind allen Mitarbeitern ihre Rollen innerhalb der Notfallorganisation bekannt?
ORG03	Sind für die verschiedenen Notfallgruppen Notfallhandbücher verfügbar und ist der Zugriff darauf gewährleistet?
ORG04	Werden alle Dokumente zur Notfallorganisation regelmäßig überarbeitet?
ORG05	Üben die Notfallteams regelmäßig den Einsatz im Notfall? Werden dabei alle Mitglieder der Notfallteams mit einbezogen?
ORG06	Werden die Ergebnisse aus den Notfallübungen dokumentiert und ermittelte Verbesserungen in die Dokumentationen eingepflegt?
ORG07	Sind alle Mitglieder des Notfallteams mit den erforderlichen technischen Gerätschaften ausgestattet?
ORG08	Sind Telefonnummern, Ansprechpartner oder E-Mail-Adressen von externen Unterstützern bekannt?

Tabelle 7.3: Checkliste Notfallorganisation



7.12.3 Checkliste Notfallpläne und Wiederanlaufpläne

NFP01	<p>Sind für alle in der Business-Impact-Analyse als kritisch eingestuften IT-Systeme Notfallpläne vorhanden?</p> <ul style="list-style-type: none"> ■ Beschreibung der Vorgehensweise bei den verschiedenen Stufen an Notfällen ■ Beschreibung der Notfallorganisation inklusive Weisungsbefugnisse ■ Kommunikationsverfahren im Notfall ■ Adress- und Telefonlisten der Mitarbeiter ■ Listen der Hersteller mit Ansprechpartnern (für die Ersatzteilbeschaffung) ■ Listen der Versicherungsunternehmen mit Ansprechpartnern ■ Beschreibung der Sofortmaßnahmen ■ Beschreibung weitergehender Maßnahmen in Abhängigkeit der Art des Notfalls ■ Klassifizierungslisten aus der Business-Impact-Analyse zur Priorisierung der Vorgehensweise
NFP02	Sind die Alarmierungslisten aktuell? Stimmen Telefonnummern und E-Mail-Adressen?
NFP03	Sind Wiederanlaufpläne für die kritischen IT-Systeme vorhanden?
NFP04	Sind die Wiederanlaufpläne auf die Prioritäten der einzelnen IT-Systeme abgestimmt?
NFP05	Sind die Besonderheiten, wie das Einschalten von Forensikern, die sich aus der Bedrohung »Cybercrime« ergeben, berücksichtigt worden?

Tabelle 7.4: Checkliste Notfallpläne und Wiederanlaufpläne

7.12.4 Checkliste Rechenzentrum

RZ01	<p>Ist im Katastrophenfall der Aufbau eines Notfallrechenzentrums vorgesehen?</p> <p>Existieren für diesen Fall entsprechende Verträge?</p> <p>Ist der Aufbau des Notfallrechenzentrums beschrieben?</p> <p>Wird der Umzug in und der Betrieb eines Notfallrechenzentrums geübt?</p>
------	---

Tabelle 7.5: Checkliste Rechenzentrum



RZ02	<p>Wurden die Risiken, die sich aus der Lage des Rechenzentrums ergeben können, erfasst und bewertet?</p> <ul style="list-style-type: none"><input type="checkbox"/> Hanglage<input type="checkbox"/> Grundwasser<input type="checkbox"/> Erdbebengebiet<input type="checkbox"/> Zufahrtswege für Rettungskräfte<input type="checkbox"/> Einflugschneise Flughafen<input type="checkbox"/> Einfluss des Klimas (Feuchtigkeit, Starkregen)
RZ03	<p>Wurde der Brandschutz in die Notfallvorsorgemaßnahmen integriert?</p> <ul style="list-style-type: none"><input type="checkbox"/> Rauch-/Brandmeldeanlage<input type="checkbox"/> Hydranten, Wasserzufuhr<input type="checkbox"/> Handfeuerlöscher<input type="checkbox"/> Löschanlage (Halon bzw. Sauerstoffreduktion)<input type="checkbox"/> Brandabschnitte<input type="checkbox"/> Kennzeichnung von Löschgerät und Meldeanlagen<input type="checkbox"/> Notausschalter<input type="checkbox"/> Kennzeichnung von ELT-Verteiler und Sicherungskästen<input type="checkbox"/> Regelmäßige Prüfung aller Brandschutzanlagen und Gerätschaften<input type="checkbox"/> Einweisung von Mitarbeitern<input type="checkbox"/> Blitzschutzanlage<input type="checkbox"/> Kennzeichnung von besonders entflammabaren Materialien<input type="checkbox"/> Entfernung von Verpackungsmaterial und anderen, nicht im RZ benötigten Stoffen
RZ04	<p>Wurde der Schutz vor Wasser in die Notfallvorsorgemaßnahmen integriert?</p> <ul style="list-style-type: none"><input type="checkbox"/> Kennzeichnung Hauptabsperrhahn<input type="checkbox"/> Schulung von Mitarbeitern in der Nutzung des Hauptabsperrhahns<input type="checkbox"/> Wasserleitung im RZ sind gesichert<input type="checkbox"/> Heizkörper im RZ sind abgesichert<input type="checkbox"/> Rückstausperre gegen Wasser aus der Kanalisation, Wassermelder

Tabelle 7.5: Checkliste Rechenzentrum (Forts.)





8 Verfügbarkeitsmanagement

8.1 Kapitelzusammenfassung

Ein weiteres Unterthema des IT Business Continuity Managements ist das Verfügbarkeitsmanagement. Bei dieser Thematik geht es darum, wichtige IT-Systeme durch technische Maßnahmen möglichst unterbrechungsfrei zu betreiben. Die Palette der Möglichkeiten reicht von RAID-Systemen über Clusterlösungen bis hin zu redundanten Rechenzentren an weit entfernten Orten. Also von der Vermeidung von Datenverlusten bis hin zur Sicherstellung, dass ein Notfall von katastrophalen Ausmaßen nicht das Ende des Unternehmens bedeutet.

Die Top-3-Fragen zum aktuellen Kapitel:

- Liegt ein Dokument vor, das definiert, welche Abstufungen an Verfügbarkeit im Rahmen von Service Level Agreements mit internen und externen Partnern Verwendung finden?
- Wurden Wartungsverträge abgeschlossen, die die vereinbarten Service Level Agreements abdecken?
- Existieren Richtlinien, die abhängig von der Wichtigkeit eines IT-Systems bestimmte technische und bauliche Maßnahmen zur Steigerung der Ausfallsicherheit vorschreiben?

8.2 Einführung

Das Verfügbarkeitsmanagement (*availability management*), auch »Kontinuitätsmanagement« genannt, trägt dazu bei, dass der IT-Betrieb störungsfrei funktioniert und eine kontinuierliche Bereitstellung wichtiger IT-Dienstleistungen sichergestellt ist. Als Bestandteil des IT Business Continuity Managements grenzt es sich vom IT-Notfallmanagement ab, das dann einspringt, wenn das Verfügbarkeitsmanagement versagt. So gesehen ist das Verfügbarkeitsmanagement das Tagesgeschäft, und das IT-Notfallmanagement dient der möglichst reibungslosen Notfallreaktion in einer Ausnahmesituation.



Das Verfügbarkeitsmanagement setzt Maßnahmen um, die zur Erreichung des Schutzzieles »Verfügbarkeit« dienen.

8.3 Richtlinie zum Verfügbarkeitsmanagement

Die Richtlinie zum Verfügbarkeitsmanagement legt die strategischen Eckpunkte fest, wie IT-Dienstleistungen und die IT-Systeme und Applikationen, von denen sie abhängen, ausfallsicher aufgebaut und betrieben werden müssen. Folgende Punkte sind dabei zu definieren:

- Eine genaue Definition des Begriffes »Verfügbarkeitsmanagement« und eine Abgrenzung zu den Themen »Service-Level-Management«, »Kapazitätsmanagement« und »Konfigurationsmanagement«. Während das »Service-Level-Management« Kennzahlen für die Messung von Servicequalität festlegt, das Konfigurationsmanagement den Betrieb der IT beschreibt und das »Kapazitätsmanagement« die Planung von Erweiterungen (*sizing*) unterstützt, kümmert sich das Verfügbarkeitsmanagement um die Sicherstellung des unterbrechungsfreien IT-Betriebs.
- Eine Strategie für das Verfügbarkeitsmanagement muss erarbeitet, etabliert und betrieben werden. Eine übergeordnete Strategie kann z.B. vorsehen, dass alle Daten einer hohen Klassifizierungsstufe grundsätzlich redundant vorgehalten werden.
- Ziele für die Verfügbarkeit von IT-Dienstleistungen müssen erarbeitet werden. Neben der allgemeinen Continuous Service Delivery Assurance (CSDA), die eine Art Selbstverpflichtung zur Bereitstellung kritischer IT-Dienstleistungen darstellt, können Service Level Agreements (SLAs) abgeschlossen werden, die detailliert Leistungen garantieren.
- Maßnahmen werden definiert, die die Sicherstellung von Verfügbarkeit gewährleisten.
- Methoden zur Überwachung der Verfügbarkeit werden festgelegt. Kennzahlen müssen erarbeitet werden, um die Qualität und die Fortschritte des Verfügbarkeitsmanagements bewerten und darstellen zu können.

Eine Richtlinie enthält auf oberster Denkebene die grundlegenden Bestimmungen, angepasst an die Unternehmensstrategie. Von diesen Definitionen ausgehend verlinken die einzelnen Punkte auf entsprechende Richtlinien auf der Arbeitsebene der IT-Mitarbeiter und der IT-Security-Organisation. So wer-



den die Maßnahmen zur Sicherstellung von Verfügbarkeit in Richtlinien definiert, die explizite technische Vorgaben machen, wie eine Umsetzung auszusehen hat.

8.4 Verfügbarkeit

Verfügbarkeit definiert sich durch die Zeitspanne, während der Systeme oder – von einer übergeordneten Ebene aus – Prozesse ihre definierten Anforderungen erfüllen. Die eingeforderte Zeitspanne wiederum wird in speziellen Service Level Agreements (SLAs) beschrieben. Ein solcher Vertrag zwischen einem Auftraggeber und einem Auftragnehmer, häufig der IT, definiert in Form von Dienstleistungsparametern, welche Verfügbarkeitsgarantien einzuhalten sind. Die darin beschriebenen Leistungen reichen von Reaktionszeiten bis hin zur Wiederherstellung von IT-Systemen oder Daten.

8

Wichtig

Die Aufstellung von Regeln, in diesem Fall niedergeschrieben in den SLAs, ist nur dann sinnvoll, wenn diese auch überprüft werden. Um dies bewerkstelligen zu können, muss Verfügbarkeit messbar gemacht werden.

Verfügbarkeit wird prozentual angegeben, und zwar als Ergebnis der gesamten Betriebszeit abzüglich der Ausfallzeit, geteilt durch die gesamte Betriebszeit.

Hinweis

Neben der Verfügbarkeit ist in der EU-DSGVO auch das Schutzziel der »Belastbarkeit« aufgenommen worden. Geht man von der englischen Fassung der EU-DSGVO aus, dann ist es als »Widerstandsfähigkeit« zu übersetzen. Diese bezieht sich nicht auf das einzelne IT-System alleine, sondern auf den gesamten Punkt-zu-Punkt-Prozess, personenbezogene Daten zu verarbeiten und zur Verfügung zu stellen. Die Unterscheidung zur Verfügbarkeit liegt darin, dass Maßnahmen nicht getroffen werden, um definierten Ereignissen, wie z.B. einem Stromausfall, durch redundante Systeme zu begegnen, sondern es geht vielmehr um die allgemeine



Widerstandsfähigkeit gegen jede Art von Schwachstellen auf dem gesamten Übertragungsweg. Das zwingt den Betreiber von Services dazu, über seinen Tellerrand zu schauen und von der Stromversorgung über den Arbeitsplatzrechner und das Netzwerk bis hin zu den Serversystemen und Datenspeichern ein sicheres Gesamtbild zu entwerfen. Die Belastbarkeit erstreckt sich damit auf die gesamte Verarbeitung eines personenbezogenen Datums und ist damit mehr als die Systeme einzeln betrachtet. Die Belastbarkeit adressiert gleichzeitig sowohl die Verfügbarkeit als auch die Integrität personenbezogener Daten.

Die Verfügbarkeit, die in SLAs geregelt wird, wird ergänzt durch die allgemeine und kontinuierliche Verpflichtung, kritische Dienste bereitzustellen. Im Fachjargon nennt man dies »Continuous Service Delivery Assurance« (CSDA).

Naturgemäß verschlechtert sich die Verfügbarkeit mit dem Ansteigen der Ausfallzeit, und deshalb ist es erforderlich, genau zu definieren, in welchen Fällen es sich um einen Ausfall handelt. Anstelle von Ausfallzeit könnte man auch von »unerwarteter Ausfallzeit« sprechen, denn geplante Zeiten wie Wartungen zählen im Normalfall nicht dazu. Anders sieht es aus, wenn mittels SLAs eine Verfügbarkeit von 7 mal 24 garantiert wird – also eine Verfügbarkeit rund um die Uhr an 365 Tagen im Jahr. In diesem Fall dürfen auch Wartungen nicht zu einer Nichtverfügbarkeit führen. Die garantierte Verfügbarkeit müsste also 100 % betragen.

8.4.1 Klassifizierung von Verfügbarkeit

Ab einer Verfügbarkeit von über 99,99 % spricht man häufig von »Hochverfügbarkeit«. In diesem Fall dürften die betroffenen Systeme jährlich bis zu maximal ca. 53 Minuten ausfallen. Möglich wird dies durch den Aufbau von redundanten Systemen, die es erlauben, Teile des Systems einer Wartung zu unterziehen, ohne den Betrieb zu stören.

Es existiert keine allgemein anerkannte Definition, ab welcher prozentualen Verfügbarkeit ein System als hochverfügbar gilt oder im Gegensatz dazu als wenig bzw. niedrig verfügbar. Trotzdem ist es sinnvoll, intern eine solche Klassifizierung festzulegen, um unternehmensweit von den gleichen Einstufungskriterien sprechen zu können.



Die Grundlage für die Berechnung sind die Annahmen, dass ein Jahr 365,25 Tage hat, jeder Monat die Länge von $\frac{1}{12}$ eines Jahres und dass jeder Tag 24 Stunden hat.

Daraus ergibt sich exemplarisch eine Verfügbarkeitsklassifizierung, die folgendermaßen aussehen könnte:

- Verfügbarkeitsklasse 1 mit 99 % Verfügbarkeit
- Verfügbarkeitsklasse 2 mit 99,5 % Verfügbarkeit
- Verfügbarkeitsklasse 3 mit 99,9 % Verfügbarkeit
- Verfügbarkeitsklasse 4 mit 99,99 % Verfügbarkeit

Auf der einen Seite muss nicht jedes System zwingend hochverfügbar sein, auf der anderen Seite ist es denkbar, dass Systeme benötigt werden, bei denen selbst eine 99,9 %ige Verfügbarkeit nicht als ausreichend erachtet wird.

Wichtig

Es muss bedacht werden, dass die tolerierte, maximale Ausfallzeit eines Systems pro Jahr auch an einem Stück eintreten kann. So stellt eine mögliche Ausfallzeit von »maximal 48 Stunden pro Jahr« über das ganze Jahr verteilt vielleicht kein Problem dar, beginnt diese aber an einem Dienstagabend und reicht bis Donnerstagabend, dann kann sie zu einem großen unternehmerischen Risiko werden. Das zeigt den oftmals sehr akademischen Wert einer solchen Betrachtungsweise.

Die Eingruppierung eines Systems in eine Verfügbarkeitsklasse kann unter Nutzung des formalen Rahmens einer Business-Impact-Analyse geschehen. Die dabei erfassten Entscheidungskriterien sind auch im Nachhinein vergleichbar und nachvollziehbar. Wichtige Kriterien, wenn man bedenkt, dass die finanziellen Folgen einer solchen Einstufung immens sein können.

Der Zusammenhang zwischen Kosten und einer Klassifizierungseinstufung ist leicht zu erkennen: Höhere Verfügbarkeit geht einher mit redundanten und damit komplexeren Implementierungen, die zudem häufig einem höheren Wartungsaufwand unterworfen sind. Auch hier gilt, dass die Kosten mit zunehmender Garantie der Verfügbarkeit überproportional steigen.



8.4.2 Vorgehensweise

Wie es der Name schon suggeriert, ist der Maßstab, an dem das Verfügbarkeitsmanagement gemessen wird, die Verfügbarkeit definierter IT-Systeme und damit der Prozesse, die von diesen unterstützt werden. Aus diesem Grund steht am Anfang zunächst die Bewertung von IT-Systemen im Rahmen der Business-Impact-Analyse, um die wichtigsten IT-Systeme zu identifizieren. Im zweiten Schritt ist es erforderlich, über Service Level Agreements für die ermittelten IT-Systeme definierte Anforderungen an deren Verfügbarkeit zu definieren. Die Anforderungen an die Verfügbarkeit sind damit eine Ableitung der Anforderungen des darüber betriebenen Service.

Die Festlegung der maximal tolerierbaren Ausfallzeiten (MTD, vom englischen *maximum tolerable downtime*) ist das Ergebnis der Business-Impact-Analyse und die Ausgangsgröße für das Verfügbarkeitsmanagement. So wie Schutzstufen können auch IT-Systeme nach einem Klassifizierungsschema bewertet werden.

Beispielhaft kann dies wie folgt aussehen:

- Stufe 1: Unkritische Systeme, MTD = 10 Tage
- Stufe 2: Wichtige Systeme, MTD = 5 Arbeitstage
- Stufe 3: Kritische Systeme, MTD = 1 Arbeitstag
- Stufe 4: Geschäftskritische Systeme, MTD = 4 Stunden
- Stufe 5: Existenziell kritische Systeme, MTD = 60 Minuten

Werden in einem Unternehmen Systeme mit einer MTD von 60 Minuten definiert, so steht von vornherein fest, dass dieser Wert bei einem Hardwareproblem nicht immer eingehalten werden kann. In einem solchen Fall müssen redundante Systeme aufgebaut werden.

Tipp

In vielen Fällen ist die Entwicklung von Notfallstrategien wie der Notbetrieb mithilfe handschriftlicher Notizen auf Papier kostengünstiger als der Aufbau von hochverfügbaren IT-Systemen. In diesem Fall könnte die MTD auf 4 Stunden erhöht werden. Ein Wert, der durch entsprechende Wartungsverträge abgesichert werden kann und der den Aufbau komplexer redundanter Systeme unter Umständen unnötig werden lässt.



Die Festlegung der MTD sollte zunächst auf Prozessebene erfolgen und danach auf alle IT-Systeme vererbt werden, die erforderlich sind, um den Prozess betreiben zu können. Dabei ist darauf zu achten, dass unterstützende Prozesse auch Beachtung finden.

8.4.3 Berechnung der Verfügbarkeit

Redundante IT-Systeme können im Notfall die Verfügbarkeit erhöhen, wobei bedacht werden muss, dass das schwächste Glied in der Kette die Gesamtverfügbarkeit bestimmt, und gerade dieses System ist vielleicht nicht ausfallsicher implementiert. Aus diesem Grund ist die Berechnung der tatsächlichen, erwarteten Verfügbarkeit eines Gesamtsystems sehr aufwendig. Den Überblick über alle Parameter zu bekommen, die ein System oder eine Software beeinflussen, ist eine große Herausforderung. Diese dann unter Nutzung von Kennzahlen zu messen und zu bewerten, stellt eine weitere Problematik dar.

Ähnlich komplex ist es, die maximal tolerierbare Ausfallzeit eines Prozesses zu definieren. Es muss aber eine Berechnungsmethode gefunden werden, die annähernd korrekte Werte liefert.

Hinweis

Einer Berechnung geht immer eine Erfassung aller beteiligten Systeme voraus. Dasjenige System, das am wenigsten Sicherheit vor einem Ausfall bietet, bestimmt dann die zu erwartende Verfügbarkeit des Gesamtkomplexes.

Ein Cluster von zwei Druckservern schützt vor Ausfall eines dieser Server. Fällt die Stromversorgung aus, so sind wiederum beide Server betroffen. Komplizierter wird es, wenn zwei Ereignisse zusammenfallen. Fällt nun gleichzeitig die Leitung zwischen den beiden Servern aus, die die Kommunikation der Art »Bist du noch da?« und »Ja, alles in Ordnung. Du musst nicht übernehmen« steuert, dann wird der Ausfall eines Servers dazu führen, dass es der andere Server nicht bemerkt, und faktisch wird der Druckdienst damit nicht zur Verfügung stehen. In beiden Fällen führen unterstützende Infrastrukturkomponenten dazu, dass Redundanzmechanismen nicht zum Tragen kommen. Eine Einschätzung, wie diese quantitativ zu bewerten sind, stellt sich außerordentlich schwierig dar.



Da die Wahrscheinlichkeit sehr hoch ist, dass die beiden eben genannten Einzelereignisse zeitlich verzögert auftreten, kann der Problematik, dass das Zusammentreffen zweier Fehler zu einem Ausfall eines redundanten Systems führt, ein Monitoring entgegengesetzt werden. In diesem Fall müssen alle Bereiche überwacht werden, die die beiden Computer systematisch unterstützen. Das würde das Netzwerk betreffen, die Kommunikationsleitung zwischen den Rechnern, die redundante unterbrechungsfreie Stromversorgung, die Stromverteiler, eventuell gemeinsame Plattenbereiche und die Computer und Dienste an sich. Aus den Daten der Überwachung lassen sich im Nachhinein zudem Informationen über die Verfügbarkeit einzelner beteiligter Komponenten ableiten.

8

8.5 Ausfallsicherheit

Ob es sich um ein Betriebssystem oder um eine beliebige andere Software handelt, potenzielle Fehlerquellen sind immer vorhanden. Die Kunst liegt darin, Software genauso wie auch Hardware in einem kontrollierbaren Zustand zu halten, der auch dann beherrschbar bleibt, wenn die fehlerhafte Routine ausgelöst wird oder ein Bauteil versagt. Dies wird natürlich maßgeblich dadurch beeinflusst, wie professionell ein Programm entwickelt und eine Hardware konzipiert wurde.

Verhält sich ein Programm anders als vom Programmierer ursprünglich vorgesehen, dann ist entscheidend, wie mit dem Fehler umgegangen wird. Im besten Fall wird er durch das Programm erkannt und durch entsprechende Algorithmen behoben. Ein Beispiel aus den alten Zeiten von Turbo Basic war die Division durch null. Da das Teilen durch null verboten ist, stürzten Programme ab, falls dies z.B. durch Fehleingaben doch vorkam. In diesem Fall wurde das Problem dadurch abgefangen, dass man vor jeder Zeile, die eine Division enthalten hat, erklärte: »Passiert nun ein Fehler, dann fange ich ihn ab und liefere als Ergebnis den Wert x«. Der Fehler konnte immer noch auftreten, nur hat er keinen Absturz mehr verursacht, und die Rechenoperation konnte ungehindert, wenn auch nicht immer mathematisch korrekt, weitergeführt werden. Das Gleiche gilt für Betriebssysteme. Fehler treten auf, und mit ihnen muss umgegangen werden. Ausfallsicherheit beschreibt damit nicht ein perfektes System, sondern den Umgang mit Fehlern.

Ein weiterer Aspekt ist die Bereinigung von Fehlern. Werden Fehler bekannt, und dazu gehören auch die bekannten Sicherheitsschwachstellen, so müssen



diese wie eben erklärt abgefangen oder aber bereinigt werden. In vielen bekannten Betriebssystemen und auch Anwendungssoftware geschieht diese Bereinigung durch täglichen Abgleich mit Datenbanken im Internet, die jeweils die neuesten Versionen bereithalten. Eine solche Möglichkeit erhöht die Ausfallsicherheit und die Verfügbarkeit.

Kenngrößen, die zur Beurteilung der Ausfallsicherheit von Software herangezogen werden können, sind zum einen die in der Vergangenheit vorgekommenen Ereignisse und zum anderen die Regelmäßigkeit von Aktualisierungen. Interne Kennzahlen lassen sich aus den Wartungsplänen für die entsprechenden Systeme ableiten. Wird ein Server monatlich auf Fehler und den Patchstand untersucht, so kann dieses Intervall zu kurz oder zu lang sein. Hier obliegt es dem Manager IT-Security, sinnvolle und dem Risiko angemessene Regelungen zu treffen.

8

8.6 Ausprägungen von Redundanz

Redundanz ist nicht einfach zu erreichen und gehört zu den technisch anspruchsvollsten Tätigkeiten innerhalb der IT. Ein System wie einen Server oder einen Core-Switch aufzubauen oder für Ausfallsicherheit durch ein redundantes Konstrukt zu sorgen, sind zwei völlig verschiedene Disziplinen. Handelt es sich um **statische Redundanz**, wenn z.B. ein Backup-System im Schrank bereitgehalten wird, dann ist bereits einiges zu bedenken. Soll es aber ein **dynamisches System** sein und der Ausfall des Primärsystems ohne Zeitverlust aufgefangen werden, dann steigt die Komplexität der Tätigkeit immens. Bereits im ersten Fall muss dafür Sorge getragen werden, dass das Backup-System jederzeit dieselben Konfigurationen etc. trägt und dass es Handlungsanweisungen gibt, wie es im Notfall eingesetzt werden muss. Im zweiten Fall kommen einige weitere Aspekte hinzu, die in den folgenden Abschnitten beschrieben werden.

Um die Verfügbarkeit von IT-Systemen durch technische und organisatorische Maßnahmen zu erhöhen, sind zuallererst die Begriffe »Redundanz«, »bauliche Maßnahmen« und »Datensicherung« zu nennen. Durch Redundanz werden technische Ausfälle von Soft- und Hardware abgefangen und z.B. durch ein parallel arbeitendes System oder alternative Prozesse ersetzt. Die Datensicherung sorgt andererseits für die Sicherstellung, dass Daten weggesichert werden, und die Wiederherstellung ist der Prozess, diese Daten wieder



verfügbar zu machen. Diese beiden Grundpfeiler bestimmen im Wesentlichen das Risiko eines Ausfalls und damit das Anlaufen des IT-Notfallmanagements. Durch bauliche Maßnahmen werden wiederum die Rahmenbedingungen geschaffen, dass die entsprechenden Gerätschaften ausfallsicher arbeiten können. Zu diesem Punkt gehören vor allem die Stromversorgung, Feuerschutzmaßnahmen und der Zugangsschutz.

Redundanz sollte aus allen Perspektiven betrachtet werden, um zu verstehen, welche Komponenten zusammenarbeiten müssen, um ein befriedigendes Ergebnis zu bekommen. Die wichtigsten Teilespekte werden »strukturelle Redundanz«, »funktionelle Redundanz« und »Informationsredundanz« genannt. Für ein funktionierendes Gesamtkonstrukt ist es erforderlich, dass die Redundanz auf allen drei Ebenen miteinander harmoniert.

8

8.6.1 Strukturelle Redundanz

Hier handelt es sich um die klassische technische redundante Auslegung von IT-Systemen. Dazu gehören RAID-Systeme, Cluster-Lösungen, ausfallsichere Netzwerke durch Parallelinstallationen und doppelt ausgelegte Notfallaggregate zur Stromversorgung. Es dreht sich also alles darum, dass, wenn ein System ausfällt, in diesem Fall ein zweites die Aufgaben übernimmt. Das zweite System hat dabei die Aufgabe, exakt dieselben Funktionen bereitzustellen wie das Primärsystem. Natürlich kann die Redundanz gesteigert werden, indem mehr als zwei Systeme genutzt werden. Man spricht dann von Clustern mit n Nodes.

Grundsätzlich wird dabei in zwei Arten von Cluster-Lösungen unterschieden: Aktiv-Aktiv und Aktiv-Passiv. Im ersten Fall arbeiten von vornherein zwei Systeme parallel, wenn eines davon ausfällt, hat das zweite aber noch genügend Ressourcen, um den Ausfall zu kompensieren. In diesem Fall können sich Parameter wie die Antwortgeschwindigkeit aufgrund der Mehrlast negativ verschieben. Diese Faktoren müssen beim Aufbau und vor allem bei der Planung berücksichtigt werden. Aktiv-Passiv werden die Systeme genannt, bei denen ein System aktiv ist und das zweite nur in Bereitschaft gehalten wird und dann einspringt, falls das erste ausfällt. In diesem Fall wird die doppelte Hard- und Software bereitgehalten, obwohl nur ein System während des Normalbetriebs produktiv ist.



8.6.2 Funktionelle Redundanz oder unterstützende Redundanz

Systeme zur funktionellen Redundanz unterstützen die strukturelle Redundanz. So reicht es nicht aus, nur zwei Server redundant aufzubauen. Für echte Redundanz müssen auch verschiedene Infrastrukturkomponenten ohne Zeitverzug einspringen können, und für dieses Verhalten sind umfangreiche zusätzliche funktionelle Techniken einzusetzen. So können zentrale Systeme überwachen, ob ein Dienst innerhalb der IT-Infrastruktur ausfällt, um dann automatisch alternative Dienste zu aktivieren.

Innerhalb eines redundanten Systems werden diese unterstützenden Funktionen als funktionelle Redundanzen bezeichnet. Zu den unterstützenden Systemen gehören damit auch das Monitoring und andere Techniken zur Ermittlung von Ausfällen.

8

8.6.3 Informationsredundanz

Alle Informationen, die über die reinen Nutzdaten hinausgehen und dazu dienen, Redundanz zu unterstützen, werden als Informationsredundanz bezeichnet. Dazu gehören z.B. die in RAID-Systemen erzeugten zusätzlichen Prüfsummen, die ausschließlich dazu dienen, bei einem Ausfall die ursprünglichen Daten wiederherzustellen. In diesem Zusammenhang ist auch von »Informations-Overhead« die Rede. Informationsredundanz ist in viele Gerätschaften automatisch integriert. Ob es sich um die Prüfbits in Speicherbausteinen oder um doppelte Zuordnungstabellen auf Festplatten handelt, immer werden Daten in einer Form ausfallsicher gehalten, indem sie mehrfach abgelegt oder mittels Prüfsummen wiederherstellbar gemacht werden.

8.7 Redundante Hard- und Software

Im Wesentlichen müssen beim Aufbau eines redundanten Systems neben den unterstützenden Systemen drei Komponenten beachtet werden: die Software, die Hardware und das Netzwerk. In Abbildung 8.1 ist der grundsätzliche Aufbau einer redundanten Hardware aufgezeigt. Die doppelte Auslegung von Bauteilen kann dabei immer weiter getrieben werden. So ist es sinnvoll, bei zwei redundanten Servern jeweils zwei eigene, wieder redundante Netzteile vorzusehen, da der Ausfall eines Netzteils unter Umständen einer höheren Wahrscheinlichkeit unterliegt als z.B. der Ausfall eines Speicherbausteins.



KAPITEL 8 – VERFÜGBARKEITSMANAGEMENT

Außerdem kann so jeder Server über redundante Leitungen mit der Stromversorgung verbunden werden. Die Alternative, einen dritten Server einzubinden, um die mathematisch erreichbare Verfügbarkeit zu erhöhen, könnte wiederum höhere Kosten verursachen, als sie durch die erhöhte Verfügbarkeit zu rechtfertigen wären. Das Beispiel soll zeigen, dass eine Betrachtung aller Komponenten erforderlich ist, um den wirtschaftlichsten Weg zu finden, die vereinbarte Ausfallsicherheit zu erreichen.

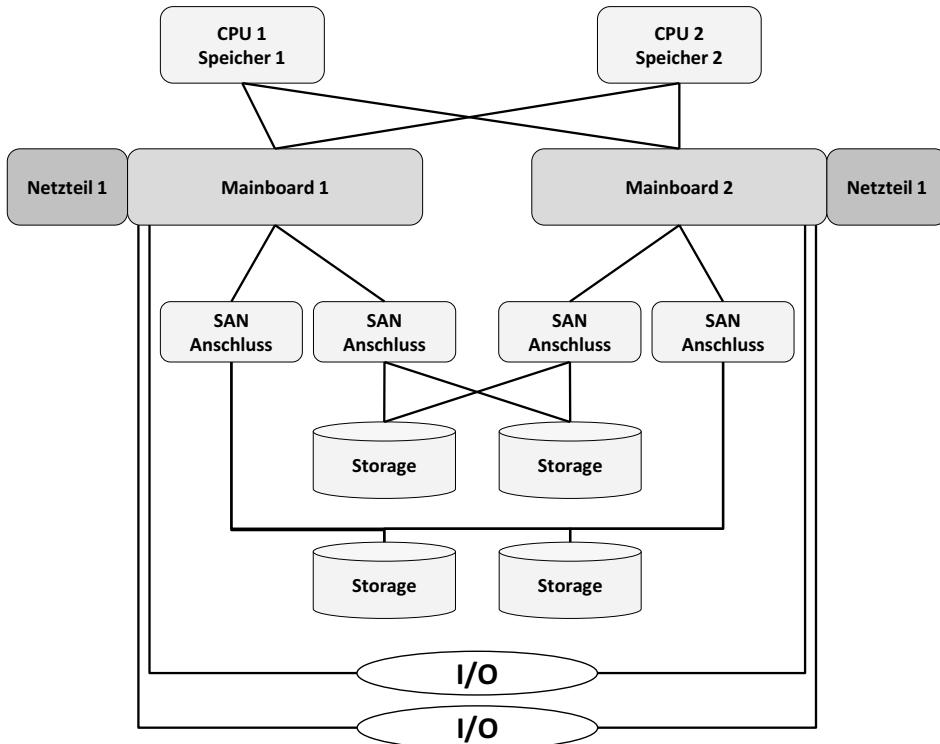


Abbildung 8.1: Redundante Bauteile

Software redundant auszulegen, ist nicht ganz so einfach, wie es bei der Hardware der Fall ist. Dies liegt vor allem darin begründet, dass Softwarefehler bzw. Falscheingaben oder fehlerhafte Daten durch verschiedene Quellen verursacht werden können und dass diese nicht immer auch als Fehler erkannt werden. So führen Falscheingaben dazu, dass auch fehlerhafte Daten auf die Datenplatten geschrieben werden. Dies kann nicht durch eine parallel installierte Software abgefangen werden. Das Gleiche gilt für den Fall, dass Soft-



ware abstürzt oder in einen unkontrollierbaren Zustand verfällt. Wurden bereits falsche Daten geschrieben oder hängt eine laufende Transaktion in der Luft, dann kann dies nicht einfach durch eine parallele Installation kompensiert werden.

An diesen Beispielen ist zu erkennen, dass es in vielen Fällen erforderlich wäre, eine weitere, übergeordnete Softwareinstanz einzuführen, die wiederum redundant aufzubauen wäre und die die Aufgabe hätte, die produktive Software zu überwachen, den Datenverkehr zu prüfen und als letzte Instanz regelnd einzutreten, falls es zu Fehlfunktionen kommt. Alle diese Argumente zeigen, warum Redundanz aufseiten von Software weniger zum Einsatz kommt und warum Software in den meisten Fällen »nur« an redundante Hardware gekoppelt ist.

8.8 Virtualisierung

Die Entkopplung von Diensten, die die IT zur Verfügung stellt, und den technischen Ressourcen liegt seit einigen Jahren im Trend und wird sich auch zukünftig immer weiter durchsetzen. Die Möglichkeit, unabhängig von der zugrunde liegenden Hardware ein komplettes Serversystem zu sichern, wiederherstellen und beliebig geografisch verschieben zu können, erzeugt völlig neue Facetten bezüglich der Sicherstellung von Verfügbarkeit.

Neben der Sicherstellung des Betriebs ist eine weitere Eigenschaft von Virtualisierung sehr interessant: die effektive Nutzung von Ressourcen wie CPU, Speicher und Plattenplatz. Schon dadurch, dass kurzfristig weiterer Plattenplatz zur Verfügung gestellt werden kann, und das ohne Systemunterbrechung, eröffnet weitere Möglichkeiten und gibt den Administratoren neue Werkzeuge an die Hand, die IT-Infrastruktur sehr viel filigraner gestalten zu können.

Neben der Virtualisierung von Hardwarekomponenten kann auch Software virtualisiert werden. Ab diesem Zeitpunkt ist eine Applikation nicht mehr fest mit einer Hardware verknüpft und kann so einem Anwender aus einer Serverfarm heraus zur Verfügung gestellt werden. Der Vorteil liegt darin, dass zum einen Redundanz mit eingebaut ist und zum anderen, dass keine Wartungsausfälle zu erwarten sind, da die Software auf einem Host der Serverfarm gewartet werden kann, während die Anwender, ob Personen oder wiederum andere Rechner, durch einen anderen Host versorgt werden.



8.9 Bauliche Maßnahmen zur Steigerung der Verfügbarkeit

Das Ziel baulicher Maßnahmen, die der Sicherstellung einer zugesicherten Verfügbarkeit dienen, ist immer, die Rahmenbedingungen des Betriebs von elektronischen Gerätschaften zu unterstützen. Dazu gehört die klimatisch korrekte Umgebungstemperatur genauso wie eine adäquate und sichere Stromversorgung. Die meisten dieser Punkte werden bereits im Rahmen der Vorsorgemaßnahmen zum IT-Notfallmanagement erläutert und deshalb an dieser Stelle nur ergänzt.

Elektronische Geräte sind auf verschiedenste Arten empfindlich. Sie können schon bei Temperaturschwanken von wenigen Grad Celsius Schäden davontragen. Durch ihre Komplexität kann der Ausfall eines winzigen Bauteils im Netzteil zu einem Brand oder mit etwas Glück nur zu einem Stromausfall führen. Jeder der beiden Fälle muss durch entsprechende Maßnahmen abgesichert werden. Das heißt, es müssen sowohl Maßnahmen zur Brandbekämpfung als auch ein redundantes Netzteil vorgesehen werden. Damit endet die Vorsorge aber nicht. Alle Geräte sind an Schaltkästen angeschlossen, die wiederum mit Sicherungen geschützt sind. Fällt der Strom komplett aus, müssen Akkus oder Notstromaggregate automatisch übernehmen. Das Gleiche gilt auch für alle anderen Komponenten. Ratten, die Netzwerkkabel im Unterboden zerbeißen, haben vielleicht schon mehr Kosten verursacht als Bauarbeiten im Rechenzentrum und eventuell freigesetzter silikathaltiger Gips, der Kurzschlüsse auf dem Motherboard von Servern auslöst oder Festplatten zerstört, weil er klein genug ist, um durch die Luftdruckausgleichfolie der Gehäuse dringen zu können. Alle diese Beispiele kommen vor und müssen zumindest mit Maßnahmen bedacht werden.

Man sollte denken, dass ein bisschen gesunder Menschenverstand und Umsicht ausreichen würden, um solchen Fehlern aus dem Weg zu gehen. Die Erfahrung zeigt aber, dass Routine der Feind der Umsicht ist und dass nur Unternehmen halbwegs auf der sicheren Seite sind, die explizite Regeln aufstellen. Regeln, dass z.B. Bauarbeiten im Rechenzentrum grundsätzlich von IT-Mitarbeitern begleitet werden müssen, sind nicht nur schriftlich zu fixieren, sondern deren Umsetzung muss auch laufend überwacht werden.

Einfacher umzusetzen sind Maßnahmen zum Zutritsschutz. Rechenzentren, die von Unbefugten nicht betreten werden können, sind zumindest vor



BAULICHE MAßNAHMEN ZUR STEIGERUNG DER VERFÜGBARKEIT

physischer Sabotage sicher. Wenn dies auch ausnahmslos geschieht und nicht immer wieder ein Stück Holz die Zugangstüre offen hält, weil es zu mühsam ist, jeweils einen IT-Mitarbeiter um Zugang zu bitten, dann ist ein erster wichtiger Schritt getan. Natürlich bedingt dies, dass auch alle wichtigen IT-Systeme im Rechenzentrum installiert sind und nicht der eine oder andere Server unter dem Schreibtisch eines Kollegen steht.

Wie in allen Fällen der Vorsorge ist auch in diesem Bereich die Sicherheit immer weiter steigerbar. Serverschränke mit eigener Klimatisierung und einbruchsicheren Türen werden hier genauso angeboten wie Gehäuse für Netzwerkkabel, deren Öffnung Alarm auslöst. Den Mittelweg zu finden zwischen Risikoabwägung und den Kosten für die Implementierung von Maßnahmen, ist auch hier die Hauptaufgabe und sollte mit Augenmaß geschehen. Formale Kriterien sind die MTD jedes Systems, die sich wiederum auf die Fakten aus der Business-Impact-Analyse (BIA) stützen. Den Zusammenhang zwischen BIA, MTD und den Maßnahmen darstellen zu können, ist in diesem Fall die wichtige und erforderliche Aufgabe der IT-Security-Organisation.





9 Technische IT-Security

9.1 Kapitelzusammenfassung

IT-Security hat immer auch etwas mit IT-technischen Fragestellungen zu tun. Das trifft selbst dann zu, wenn die IT-Security-Organisation der Unternehmensleitung berichtet und wenn deren definierte Hauptaufgabe in der Richtlinienkompetenz und der Überprüfung von Vorgaben liegt. Wissen über die IT-Infrastruktur und die IT-Prozesse ist wichtig, um passende und praktikable Vorgaben festlegen zu können. Nur wenn der Manager IT-Security weiß, wie die Datenströme aussehen und welche IT-Systeme eine maßgebliche Rolle spielen, kann er Risiken zutreffend einschätzen und zielgerichtete Maßnahmen definieren. Dazu kommt, dass er in der Zusammenarbeit mit dem Datenschutzbeauftragten, der internen Revisionsabteilung und häufig auch mit dem IT-Leiter den Part einer beratenden Stelle einnimmt. Um diese Aufgabe adäquat leisten zu können, muss er sich intensiv mit der zugrunde liegenden Thematik auseinandergesetzt haben.

Hinweis

Vor allem in größeren Unternehmen gibt es häufig eine klare Trennung der Rollen »Richtlinienhoheit« und »Audit«, sprich IT-Security, von der technischen Umsetzung der Sicherheitsvorgaben. Dies ist vergleichbar mit den Prinzipien der Gewaltenteilung. Um bei diesem Beispiel zu bleiben, würden der IT-Security die Rollen Legislative und Judikative zukommen und dem Bereich der operativen Sicherheit die der Exekutive. Mit dieser Trennung vermeidet man, dass diejenige Instanz, die die Vorgaben macht, diese auch umsetzt und anschließend im Rahmen eines Audits bewertet. Der operativen Sicherheit kommt demzufolge auch eher der technische Part der Security zu. Nichtsdestotrotz wird auch in dieser Gemengelage die IT-Security die gewählten Maßnahmen abschätzen und die geplante Sicherheitsarchitektur bewerten müssen. Also auch in dieser Konstellation ist es erforderlich, technisch auf dem aktuellen Stand zu sein.



In diesem Kapitel werden zunächst die für uns maßgeblichen technisch-organisatorischen Maßnahmen behandelt, wie sie im Bundesdatenschutzgesetz-Neu aufgeführt sind. An diesen werden die grundlegenden technischen Fragestellungen erläutert. Anschließend folgen einzelne Themenbereiche, auf die ein Manager IT-Security in seiner Arbeit immer wieder stoßen wird.

Die Top-5-Fragen zum aktuellen Kapitel:

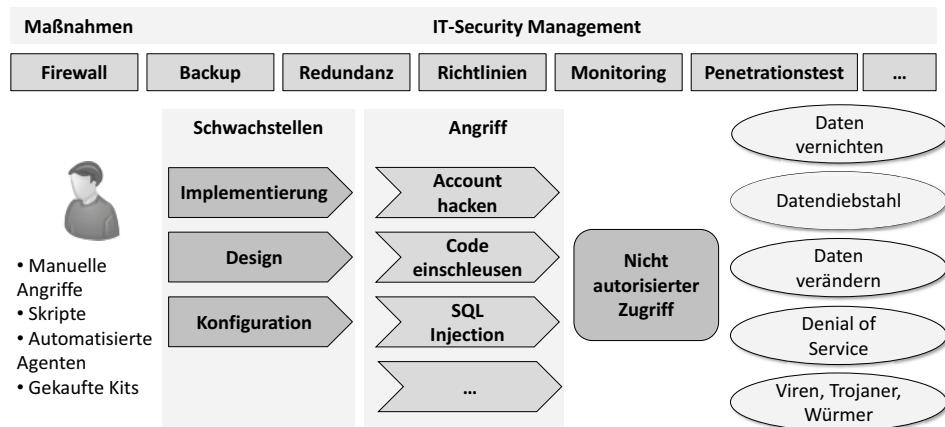
- Werden Entscheidungen dokumentiert, die der Manager IT-Security im Rahmen seiner Aufgaben trifft? Dazu gehören alle Maßnahmen und Ausnahmeregelungen und die jeweiligen Randbedingungen. Ein Beispiel wäre die Akzeptanz einer Ausnahmeregelung bezüglich der Installation einer ansonsten durch Richtlinien untersagten Software auf einem Arbeitsplatzrechner oder die Freigabe eines ungesicherten Downloads aus dem Internet.
- Sind für die einzelnen technischen Aufgabenfelder entsprechende Richtlinien vorhanden?
- Ist der Umgang der Mitarbeiter mit den Medien E-Mail und Internet geregelt?
- Ist ein Prozess beschrieben, der dann greift, wenn ein Mitarbeiter ausscheidet und ein Zugriff auf seine E-Mail-Daten und anderen (persönlichen) Daten erforderlich wird?
- Werden exponierte IT-Systeme regelmäßig in Bezug auf sicheres Betriebssystem, sichere Software und sichere Schnittstellen geprüft? Das betrifft im Besonderen alle IT-Systeme in einer »Demilitarisierten Zone« (DMZ), also Systeme, auf die aus dem Internet heraus zugegriffen wird.

9.2 Einführung

Viele Aufgabengebiete der IT-Security-Organisation beschäftigen sich mit Prozessen, mit IT-Risikomanagement oder schlicht mit der Verfolgung von Projekten. Zu diesem Komplex gesellt sich nun der technische Aspekt der IT-Security. Auch wenn die technische Expertise, die ein Manager IT-Security aufweisen muss, in den letzten Jahren im Zuge der Herausbildung von Spezialdisziplinen innerhalb des Datensicherheitskomplexes zurückgegangen ist, wird er auch aktuell und in der Zukunft nicht in der Lage sein, adäquate Vor-



gehensweisen zu definieren, ohne ein Grundverständnis für die technischen Zusammenhänge innerhalb der IT zu besitzen. Dazu kommt, dass er zum einen den sicheren Betrieb von IT-Systemen überwachen muss und zum anderen häufig selbst IT-Systeme verantworten oder sogar betreiben muss. Führt er dazu eigene Audits durch, so erweitern sich die Anforderungen weiter.



9

Abbildung 9.1: Technische Maßnahmen zur Abwehr von Angriffen

Ein typisches Beispiel ist der Manager IT-Security, der auf der einen Seite die Serverfarm auf Schwachstellen prüft, die von der IT-Abteilung betrieben wird, und technische Richtlinien zu deren Betrieb erlässt, und auf der anderen Seite eine Firewall administriert. Selbst wenn der administrative Teil wegfällt, bleibt immer noch die Erforderlichkeit bestehen, zumindest die Grundaspekte dieser Tätigkeit zu verstehen.

Hinweis

Ein Manager IT-Security kann nicht alle technischen Bereiche der IT beherrschen. In zunehmendem Maße muss er deshalb die Unterstützung interner und externer Berater in Anspruch nehmen. Das erfordert eine starke Vernetzung, vor allem mit den internen IT-Bereichen.

Auch wenn es technisch wird, muss sich der Manager IT-Security dennoch bemühen, möglichst formal an Aufgabenstellungen heranzugehen. So ist es



problematisch, wenn er sich ohne Vorgehensmodelle und vorgefertigte Prüfkataloge an die Bewertung von IT-Systemen wagt. Eine Fehlkonfiguration, die ihm an einem Server auffällt, wird ihm dann zwei Wochen später an einem anderen Server unter Umständen entgehen. Dazu kommen die Zweifel, ob er in jedem Fall eine so umfassende Prüfung vorgenommen hat, dass er ein qualifiziertes Urteil abgeben kann: »Ja, dieser Server ist sicher.«



Abbildung 9.2: Perspektiven technische IT-Security

9

Es ist hilfreich, im Vorhinein festzulegen, aus welchen Perspektiven eine technische Begutachtung von IT-Systemen stattfinden soll. Im Folgenden stellen wir zum einen die Betrachtung aus der sogenannten technisch-organisatorischen Perspektive vor. Diese ist maßgeblich aus dem Bundesdatenschutzgesetz-Neu und den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) abgeleitet und beschreibt, welche Kontrollebenen es bei der Betrachtung von Daten, Servern oder IT-Systemen gibt. Innerhalb jeder dieser Ebenen kommt irgendwann der Zeitpunkt, bei dem sich die Sicht auf technische Aspekte wie die Konfiguration von Software über die Überprüfung von Schnittstellen bis hin zur Ermittlung von Schwachstellen auf niedriger TCP/IP-Ebene verschiebt.

9.3 Technisch-Organisatorische Maßnahmen

Eine gute Übersicht über das, was von der IT-Abteilung und im Speziellen von der IT-Security hinsichtlich des Schutzes von Daten erwartet wird, liefert das Bundesdatenschutzgesetz-Neu. In § 64 werden die Maßnahmen aufgelistet, die zum Schutz von personenbezogenen Daten umgesetzt werden müssen. Für den Manager IT-Security dienen sie als Richtschnur für seine Vorgehensweise, und zusätzlich vereinheitlichen sie die Sprachregelung. Daneben wer-



den der Grad der geforderten Umsetzung und eine Richtschnur, nach der man vorgehen kann, aufgeführt. Die beiden wichtigsten Stichpunkte stammen dabei aus § 64 (1). Zunächst wird definiert, dass sich jede technische Regelung am »Stand der Technik« orientieren muss. Auf den ersten Blick erscheint dies schwammig und schwer zu fassen. Auf den zweiten Blick wird aber klar, dass sich ein Unternehmen nicht auf den umgesetzten Maßnahmen ausruhen darf, sondern ständig nachrüsten muss, um den Anforderungen zu genügen. Wie dies im Einzelnen aussehen soll, wird die Rechtsprechung noch aus definieren müssen. Selbst einige Zeit, nachdem das Gesetz vollständig in Kraft getreten ist, sind hier heute noch viele Fragen offen.

Am Ende des Absatzes steht ein weiterer wichtiger Hinweis: »Der Verantwortliche hat hierbei die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik zu berücksichtigen.« Diese Aussage relativiert den unpräzisen Charakter des Ausdrucks »nach dem Stand der Technik« weiter. Zum mindesten in Deutschland fährt man also gut, wenn man die Vorgaben, die das BSI erlässt, verinnerlicht, als verbindliche Vorgabe versteht und auch in diesem Sinne umsetzt.

Wichtig

Die nachfolgend aufgeführten Themenbereiche stammen in dieser Zusammenstellung aus dem Bundesdatenschutzgesetz-Neu. Im Zusammenhang mit dem vorliegenden Buch dienen sie, über den Schutz personenbezogener Daten hinausgehend, als Basisthemen für alle Arten von Informationen. Damit schließt sich der Kreis zwischen der rechtlichen Basis und den Anforderungen an den allgemeinen Schutz kritischer Daten, wie sie die ISO 27001 oder das BSI verfolgen.

Es ist zu beachten, dass der Datenschutzbeauftragte hinsichtlich dieser Maßnahmen eine Kontrollfunktion wahrnimmt und die Aufgabe hat, auf deren Umsetzung hinzuwirken. Die Evaluierung und Umsetzung von Maßnahmen liegt im Aufgabenbereich der Sicherheitsbereiche und dabei unter anderen bei der IT-Security-Organisation. Die letzte Verantwortung liegt wieder bei der Unternehmensleitung.



9.3.1 Zugangskontrolle

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte.

In der Neufassung des Bundesdatenschutzgesetzes wurden die Kontrollen »Zutritt« und »Zugang« zu einer Maßnahme zusammengefasst. Die Unterscheidung von »Zugang« von »Zugriff«, wobei der Zugang zu einem IT-System jetzt schon bei dem Betreten z.B. des Rechenzentrums beginnt, fällt damit weg.

Es gibt allerdings aus Sicht der Informationssicherheit auch gute Gründe, die Unterscheidung zwischen »Zutritt« und »Zugang« beizubehalten, und das werden wir in diesem Kapitel auch tun. Der Grund liegt im Umfang der Aufgaben der Informationssicherheit. Der Schutz eines IT-Systems kann sich nämlich auf mehrere Organisationseinheiten erstrecken. Häufig zu beobachten ist zum Beispiel, dass die Verantwortung für die Lage, den Außenschutz und auch den Zutritt zu einem Rechenzentrum bei der Gebäudesicherheit liegt und die IT-Security erst für den Innenraum zuständig zeichnet. In einem solchen Fall ist zwischen dem physischen Zutritt zum Raum, in dem das Rechenzentrum liegt, und dem Zugang zur Bedienungsoberfläche eines Servers zu unterscheiden. Da diese Unterscheidung durchaus Sinn macht, hat sich im Englischen der Begriff »physical access« durchgesetzt – gleichzusetzen mit dem deutschen Begriff »Zutritt«.

Zutrittskontrolle

Der Koordination des physischen Schutzes von IT-Systemen muss ganz besondere Aufmerksamkeit gewidmet werden, da dieses Thema durch unterschiedliche Sicherheitsbereiche innerhalb eines Unternehmens wahrgenommen wird. Verantwortlichkeiten sind häufig diffus und von überschneidenden Zuständigkeiten geprägt. Der äußere Perimeter, der Schutzaun, die Außenmauern und die Ausweiskontrolle werden üblicherweise vom Werksschutz gesichert. Die Verantwortung, dass kein Unbefugter das Unternehmen betritt, liegt somit zunächst einmal dort. Eine Reihe von Regelungen, wie, dass ein Externer dennoch regelkonform das Gebäude betreten darf, z.B. als Gast in Begleitung eines Mitarbeiters, führt dazu, dass die Verantwortung in diesem Fall an den begleitenden Mitarbeiter übergeht. Dieser ist für diese Arbeit aber nicht ausgebildet und wird sie auch nur in den seltensten Fällen



aktiv wahrnehmen. Damit ist nicht mehr auszuschließen, dass ein Guest unkontrolliert ihm zugängliche Bereiche betreten kann.

Ein weiterer Perimeter ist das Rechenzentrum und eventuell vorgelagerte Sicherheitsschleusen, in dem die IT-Systeme angesiedelt werden, auf denen Daten gespeichert sind. Neben Servern und Speichersystemen sind auch die Datensicherungsgerätschaften in gesicherten Räumlichkeiten unterzubringen. Die Verantwortung für bauliche Maßnahmen wird zumeist vom Gebäudemanagement oder der Gebäudesicherheit wahrgenommen und sollte in enger Abstimmung mit der IT-Abteilung und der IT-Security-Organisation stattfinden.

Typische Maßnahmen zur Sicherung des Geländes und von Gebäuden:

- Das Gelände ist in sich geschlossen und durch Mauern oder Zäune gesichert.
- Nachts wird das Gelände beleuchtet.
- Der Werkschutz führt regelmäßig Kontrollgänge durch, deren Frequenz von Außenstehenden nicht erkennbar ist.
- Mittels Kamerasystemen wird die Außenumgebung überwacht.
- Einbruchmeldeanlagen sind installiert und werden regelmäßig gewartet und getestet. Die Alarmierungskette geht direkt zu einem rund um die Uhr besetzten Sicherheitsdienst oder zur Polizei.
- Von außen, und das beinhaltet auch den Gebäudeinnenflur, zugängliche Fenster und Türen sind gesichert. Entsprechende Anforderungen können in den Standards DIN V ENV 1627 bis 1630 nachgelesen werden. Es ist sinnvoll, Fenster und Türen so zu sichern, dass sie einem Einbruchsversuch mindestens so lange standhalten, wie es durchschnittlich dauert, bis nach der Alarmierung Kräfte vor Ort sind.
- Weitere Zugänge wie Dachluken, Schächte, Zufahrten oder Kellerfenster sind gesichert.

Maßnahmen, den Zutritt zum Gebäude betreffend:

- Jede Person, die Zutritt verlangt, wird überprüft. Bei Angestellten geschieht dies durch Vorzeigen des Mitarbeiterausweises oder die Benutzung einer automatisierten Personenvereinzelungsanlage. Gäste melden



sich an der Pforte an. Die Beschäftigten dort organisieren dann das Abholen durch einen Mitarbeiter des Unternehmens.

- Vereinzelungsmaßnahmen dienen dazu, dass Personen nicht im Pulk das Gebäude betreten und Unbefugten die Chance eröffnen, sich unerkannt einzuschmuggeln. Der Pförtner hat jederzeit Sichtkontakt zu Personen, die das Gebäude betreten wollen.

Maßnahmen innerhalb des Gebäudes und in sensiblen Bereichen:

- Der Zutritt zu sensiblen IT-Systemen muss gesondert gesichert sein.
- Nur dazu autorisierte Personen erlangen Zutritt und benötigen dafür einen Ausweis. Zur Zutrittskontrolle sind Ausweis- oder Chipkartenleser zu installieren. Der Zutritt wird aufgezeichnet und dokumentiert.
- Gäste müssen stets in Begleitung sein.
- In Bereichen hoher Sicherheitsstufe sind auch Reinigungskräfte nur zu normalen Arbeitszeiten und in Begleitung zugelassen.

9

In welchem Umfang diese Maßnahmen umgesetzt werden, hängt in erster Linie davon ab, welcher Klassifizierungsstufe die zu schützenden Daten zugeordnet sind und wie sich die Sicherheit des Gebäudezugangs im Vergleich mit der Sicherung der Räumlichkeiten, in denen sich die IT-Systeme befinden, verhält. Werden beispielsweise Daten auf den Arbeitsplatzrechnern der Mitarbeiter gespeichert und lässt sich der Zutritt zu diesen Rechnern innerhalb des Gebäudes nicht ausreichend einschränken, so wird der Zutritt zum Gebäude an Wichtigkeit gewinnen. Werden ausschließlich Terminals eingesetzt und befinden sich alle Daten in einem stark gesicherten Rechenzentrum, so verhält es sich umgekehrt: Das Augenmerk wird dann beim Schutz des Rechenzentrums liegen.

Grundsätzlich kann der Vorgang weiter professionalisiert werden, indem Personen Sicherheitsfreigaben zugewiesen werden. Eine Reinigungskraft, die nach einem Background-Check eine hohe Sicherheitsfreigabe erhält, kann dann auch ohne Begleitung durch eine weitere Person Bereiche betreten, die ihrer Freigabestufe entsprechen.

Zugangskontrolle

Nachdem der physische Zutritt zu Rechenzentren und IT-Systemen im Rahmen der Zutrittskontrolle behandelt wurde, geht es bei der Zugangskontrolle



nun darum, dass nur befugte »Subjekte« Systeme nutzen können. Es dreht sich im Grunde um die Identifikation und die Authentifikation von Personen, Systemen oder auch Applikationen. Der Schwerpunkt im Datenschutz liegt auf der Subjektgruppe »Personen«, und auch im Rahmen des IT-Security-Managements wird man sich darauf konzentrieren können. Trotzdem darf man nie vergessen, dass jede Art von Subjekt, das sich Zugang verschaffen möchte, einer Identifikations- und Authentifikationsprüfung unterzogen werden muss.

Hinweis

Bei der Zugangskontrolle geht es nicht um die Autorisierung, also die Zuweisung von Zugriffsrechten. Dieses Gebiet wird von der Zugriffskontrolle abgedeckt.

9

Maßnahmen, die aus dem Themenbereich Zugangskontrolle stammen:

- Der Zugang zu einem Rechner, also die Anmeldung am Betriebssystem oder einer Software, geschieht über Mechanismen, die sicherstellen, dass der Benutzer einwandfrei identifiziert wird und dass dieser auch berechtigt ist, zuzugreifen. Deshalb findet zunächst die Identifikation, z.B. über eine Benutzer-ID statt und danach die Authentifikation, z.B. mittels eines Kennworts.
- Regelungen zur Identifikation müssen vorhanden sein. Diese regeln die technische Methode der Identifikation über ID, Smartcard oder Hardware-Token.
- Eine Richtlinie zur Erstellung sicherer Kennwörter muss vorhanden sein. Dazu gehören die Mindestlänge, die erforderliche Stärke (mit Sonderzeichen, Zahlen, Groß- und Kleinbuchstaben) und die Frequenz, in der sie geändert werden müssen.
- Der Benutzerzugang kann gesperrt werden, wenn ein Kennwort mehrmals falsch eingegeben wurde.
- Richtlinien zum Umgang mit Kennwörtern verbieten die Weitergabe und das Ablegen an unsicheren Stellen. Auch die IT-Abteilung hat üblicherweise kein Recht, Kennwörter zu verlangen. Ist dies aber unabdingbar, z.B. zur Neuinstallation eines Rechners, so ist das Kennwort direkt im Anschluss an diese Tätigkeiten vom Benutzer wieder zu ändern.



KAPITEL 9 – TECHNISCHE IT-SECURITY

9

- Die Vergabe von Kennwörtern muss geregtelt sein. Genauso wie das Zurücksetzen, falls es vom Benutzer vergessen wurde. In diesem Fall muss sich der Benutzer einwandfrei identifizieren können. Dies kann durch Vorlage eines Lichtbildausweises geschehen. Nicht jede Authentifizierungsme-thode ist gleich sicher. Weist sich ein Benutzer, z.B. um sein Passwort zurücksetzen zu lassen, per Mitarbeiterausweis ohne Foto aus, so ist dieser Vorgang unsicherer, als wenn er dies mit dem Personalausweis tut. Hier spricht man von verschiedenen »Levels of Assurance« (LoA).
- Benutzer müssen regelmäßig über den korrekten Umgang mit Kennwörtern informiert und geschult werden.
- Verlässt ein Benutzer das Unternehmen, so ist der Benutzerzugang umgehend zu sperren.
- Die Übertragung von Kennwörtern über das Netzwerk muss sicher sein. So sollte beim Zugang von außen ein verschlüsselter VPN-Zugang eingesetzt werden.
- Geeignete Antivirenprogramme müssen installiert sein, um zu verhindern, dass Schadsoftware Zugangsdaten entwenden oder sonstigen Schaden anrichten kann.
- Der Zugang zu IT-Systemen muss durch Firewalls und durch verschlüsselte Datenübertragung geschützt werden.
- Der Zugriff auf Netzwerkkomponenten muss durch entsprechende abgeschlossene Schränke reglementiert werden.
- Der Zugang über Wireless-Zugänge muss stark abgesichert werden.
- Datenübertragungen sollen grundsätzlich verschlüsselt erfolgen. Verlassen Daten das Unternehmen, z.B. über das Internet, dann ist eine Verschlüsselung Pflicht.
- Mobile Endgeräte wie Laptops, Mobiltelefone oder Kameras müssen, sofern darauf sensible Daten abgelegt sind, durch Verschlüsselung geschützt werden.

Die Überprüfung dieser Maßnahmen ist ein wichtiger Bestandteil des IT-Security-Managements. Im Gegensatz zu den eher statischen Vorkehrungen der Zutrittskontrolle sind die Maßnahmen der Zugangskontrolle ständigen Änderungen unterworfen. Insbesondere der technische Fortschritt zwingt die



IT-Security-Organisation zum stetigen Dazulernen und zur Weiterentwicklung dieser Vorgaben.

9.3.2 Zugriffskontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

Die Zugriffskontrolle regelt, welches Subjekt, Benutzer, Applikation oder ein anderes System in einem IT-System auf welches Objekt zugreifen darf. Nachdem die Zugangskontrolle sichergestellt hat, dass der richtige Benutzer oder auch das richtige System zugreifen möchte und dies durch die Prozedur der Authentifizierung auch sichergestellt wurde, muss im Rahmen der Zugriffskontrolle entschieden werden, auf welche Ressourcen der Zugriff erfolgen darf. Neben dem Zugriff sind auch alle Themen der Sicherstellung der Integrität von Daten von Bedeutung. Das umfasst alle Kopiervorgänge, manuelle und automatisierte Änderungen und Löschvorgänge. Um dies sicherstellen zu können, sind detaillierte Zugriffsregelungen zu definieren und technisch umzusetzen. Abgeleitet werden Zugriffsrechte dabei grundsätzlich von den Zugriffserfordernissen, die aufseiten eines Subjekts bestehen. Das bezeichnet man als Need-to-know-Prinzip. Diese Anforderungen ergeben sich aus den Tätigkeiten, die z.B. ein Benutzer im Rahmen seiner Arbeit abarbeiten muss. Es gilt hier die Regel, dass grundsätzlich nur die Zugriffsberechtigungen erteilt werden dürfen, die absolut benötigt werden. Das gilt auch dann, wenn es sich beim Subjekt um ein IT-System handelt. Auch in diesem Fall ist der Zugriff so weit wie möglich zu beschränken, ohne die Funktionalität zu beeinträchtigen. Ist der Zugriff nur temporär erforderlich, wie es z.B. bei einem »Notfall-Account« der Fall ist, dann ist auch nur temporär der Zugriff zu gewähren. Es sind zahlreiche Softwareprodukte vorhanden, um dies automatisiert und vollständig dokumentiert umsetzen zu können.

Die Grundlage für jede Zugriffskontrolle ist eine entsprechende Entscheidung für ein konzeptionelles Vorgehen, das mit einer Richtlinie formal untermauert wird. Davon wird die technische Umsetzung abgeleitet. Zur effektiven Erstellung und Umsetzung ist es erforderlich, zu wissen, welche Objekte und welche Subjekte betrachtet werden müssen. Eine schematische Aufstellung von Daten, Servern, Applikationen, Druckern und anderen Objekten ist also



genauso erforderlich wie eine Aufstellung aller Benutzer, am besten in Rollen zusammengefasst, Schnittstellen und IT-Systeme, die darauf zugreifen müssen. Auch die Klassifizierung und Einstufung nach Schutzstufen ist ein erforderlicher Schritt, um jeweils angepasst die korrekten Maßnahmen implementieren zu können.

Wichtig

Der Zugriff auf Objekte ist über den gesamten Lebensweg (*Date-Life-Cycle*) zu betrachten. So ist z.B. bei Entwicklungsdaten nicht nur der Zugriff auf die Daten auf dem Datenserver zu betrachten, sondern auch auf die Datensicherungsbänder, die Archivierung oder der Transport per E-Mail.

9

Zusammengefasst sind unter anderen die folgenden Maßnahmen umzusetzen:

- Eine Richtlinie sollte existieren, die beschreibt, wie der Zugriff auf definierte Daten grundsätzlich geregelt wird. Dazu gehören Zugriffskontrollmodelle und deren Umsetzung: die Methoden der Zugriffskontrolle.
- Ein Berechtigungskonzept regelt die Vergabe von Berechtigungen und unterstützt deren Verwaltung. Dieses Konzept muss den gesamten Weg von der Einstellung eines Mitarbeiters, während der Anstellung und nach dem Ausscheiden regeln. Aus diesem Grund müssen die erteilten Rechte regelmäßig hinterfragt und angepasst werden.
- Eine Übersicht über Personen, Schnittstellen, IT-Systeme und Applikationen (Subjekte), die auf Objekte zugreifen wollen, muss existieren. Dies können Benutzerlisten, ein Auszug aus dem Assetmanagement und eine Liste der vorhandenen Datentypen sein. Es empfiehlt sich, Datentypen zu kategorisieren und in Gruppen zusammenzufassen.
- Auf Basis des Berechtigungskonzepts und der vorhandenen Listen an Objekten und Subjekten müssen die vergebenen Berechtigungen überprüft werden.
- Verlassen Daten den Einflussbereich des Unternehmens, so ist Sorge dafür zu tragen, dass der Zugriff für Unbefugte weiterhin ausgeschlossen ist.



Das betrifft sowohl die Übertragung per Internet und die Übergabe von Daten an Dritte als auch die Entsorgung von Datenträgern.

- Es ist sicherzustellen, dass die im Berechtigungskonzept beschlossenen Grundsätze eingehalten werden. Dies ist nur möglich, wenn die dort festgelegten Zugriffsrechte nicht ausgehebelt werden können. Dies beinhaltet die technische Umsetzung von Maßnahmen, die den Diebstahl und die Weitergabe erschweren. Zu diesen Maßnahmen zählt das Verbot von CD/DVD-Brennern, das Scannen von E-Mail-Anhängen, der restriktive Zugang zum Internet und das Sperren von USB-Ports an den Arbeitsrechnern, um den Anschluss von externen Datenträgern zu verhindern.
- Der Zugriff auf Daten außerhalb der Arbeitszeit und von Orten außerhalb des Unternehmens muss geregelt werden, um den Abfluss von Daten zu vermeiden.

Der Zugriff auf sensible Daten sollte protokolliert werden. Damit ist nachträglich feststellbar, wer welche Daten zu welchem Zeitpunkt gelesen, gelöscht oder verändert hat. Das bezieht sich sowohl auf Dateien in Dateisystemen als auch auf Inhalte von Datenbanken.

9.3.3 Übertragungskontrolle und Transportkontrolle

Übertragungskontrolle

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

Transportkontrolle

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt wird.

Die Übertragungskontrolle soll sicherstellen, dass immer bekannt ist, an welchen Stellen personenbezogene Daten zur Verfügung gestellt werden. Dies hat viel mit Dokumentation von Schnittstellen und der Verarbeitung personenbezogener Daten im Allgemeinen zu tun. Die Transportkontrolle wiederum kümmert sich um die Übermittlung dieser Daten innerhalb eines Netz-



werks und über Netzwerkgrenzen hinweg. Dabei ist es unerheblich, wie dieser Transport technisch durchgeführt wird. So spielt das Verschicken von Informationen per E-Mail im Rahmen der Transportkontrolle eine große Rolle. Außerdem betrifft es in starkem Maße den Datenaustausch mit Dritten. Werden Daten mittels Datenträger ausgetauscht, dann kommt als weitere Kontrolle die »Datenträgerkontrolle« in das Spiel. Über den eigentlichen Schutz der Daten auf Datenträgern hinweg greift diese Maßnahme auch alle anderen Schutzziele auf. So sollen Datenträger vor Löschung, Veränderung, Diebstahl oder schlicht vor Manipulation geschützt werden.

9

Für alle Arten der Datenübertragung und den Schutz von Wechseldatenträgern sind technische Lösungen wie die Verschlüsselung, dedizierte Leitungen, verschlüsselte VPN-Zugänge oder Datenaustauschserver, die auf sicheren Transportprotokollen basieren, auf dem Markt. Nicht in jedem Fall wird ein großer und damit auch teurer Aufwand getrieben werden müssen. Welche Maßnahme eingesetzt werden muss, hängt auch in diesem Fall vom Schutzbedarf der zu übertragenden oder zu transportierenden Informationen ab. Hilfreich ist ein Regelwerk, das für jedes Medium und für jede Schutzstufe eine bestimmte technische Lösung vorschreibt. In der nachfolgenden Tabelle ist ein solches Regelwerk exemplarisch dargestellt.

Lfd. Nr.	Übertragungsweg	Stufe	Maßnahme
Ü01	E-Mail	Schutzstufe 1	Die Übertragung kann ohne weiteren Schutz erfolgen.
		Schutzstufe 2	Die zu übertragenden Daten (Attachment) müssen mit einem Packprogramm gepackt und per AES verschlüsselt werden. Die minimale Passwortlänge beträgt 12 Zeichen und muss per Telefon übermittelt werden.
		Schutzstufe 3	Für die Übertragung ist ein Verschlüsselungs-Gateway (eine Instanz in der E-Mail-Kette, die E-Mail verschlüsselt) zu nutzen. Das Verfahren ist PGP, und im Voraus muss ein Austausch von Schlüsseln stattgefunden haben.



TECHNISCH-ORGANISATORISCHE MAßNAHMEN

Lfd. Nr.	Übertragungs-weg	Stufe	Maßnahme
Ü02	Postweg	Schutzstufe 1	Daten auf USB-Sticks oder CD/DVD können gut verpackt auf dem normalen Postweg, als Paket, versichert und damit nachverfolgbar gemacht, versendet werden.
		Schutzstufe 2	Daten auf USB-Sticks oder CD/DVD müssen verschlüsselt werden (AES 256 Bit und einem Passwort von >11 Zeichen) und können gut verpackt, auf dem normalen Postweg, als Paket, versichert und nachvollziehbar versendet werden.
		Schutzstufe 3	Daten auf USB-Sticks oder CD/DVD müssen verschlüsselt werden (AES 256 Bit und einem Passwort von >11 Zeichen) und können gut verpackt, auf dem normalen Postweg, als Wertbrief, versichert und nachvollziehbar versendet werden.
Ü03	Internet	Schutzstufe 1	Der unverschlüsselte Upload oder Download per FTP ist in angemeldeten Einzelfällen gestattet. In jedem Fall wird überprüft, ob nicht alternativ eine sichere Übertragung zur Verfügung steht. Die Übertragung per HTTPS wird HTTP oder FTP vorgezogen.
		Schutzstufe 2	Der Upload oder Download per FTP ist verboten. Alternativ kann die sichere Alternative SFTP genutzt werden. Der Upload oder Download per HTTPS ist gestattet, sofern auf der Partnerseite ein gültiges Zertifikat nachgewiesen werden kann.
		Schutzstufe 3	Der Upload oder Download über das Internet ist nur über ein sicheres VPN gestattet.



KAPITEL 9 – TECHNISCHE IT-SECURITY

9

In der Tabelle ist zu erkennen, dass zur jeweiligen Problemlösung eine Mischung aus IT-Infrastruktursystemen wie einem Verschlüsselungs-Gateway für E-Mail auch einfache Lösungen wie z.B. ein geeignetes Packprogramm mit Verschlüsselungsoption angeboten werden. Damit ist eine Umsetzung auch in kleineren Unternehmen möglich. Neben dem technischen Angebot müssen die Vorgaben dann noch kommuniziert, verbindlich vorgeschrieben und mit den entsprechenden Anleitungen versehen werden. Insbesondere der letzte Punkt ist sehr wichtig, da auf die Selbstständigkeit des einzelnen Mitarbeiters vertraut werden muss und ein fehlendes Häkchen im entsprechenden Programm bereits den kompletten Schutz aushebeln kann. Da Passwörter verloren gehen und es auch Firmen gibt, die sich nicht per PGP, TLS oder S/MIME anbinden lassen, sind zu den technischen Rahmenbedingungen auch die jeweiligen Prozesse und Dienstleistungen zu erarbeiten, die dem Unternehmen helfen, sich strukturiert auf solche Gegebenheiten vorzubereiten und Lösungen anzubieten.

Die Weitergabe von Daten innerhalb eines Unternehmens ist ein weiterer wichtiger Punkt, der beachtet werden muss. Über interne öffentliche Netzlaufwerke, öffentliche Postkästen oder das Intranet werden häufig Daten zwischen Abteilungen ausgetauscht. Die Standardeinstellung, dass jeder schreiben und lesen darf, führt dann schnell dazu, dass dort Dokumente abgelegt werden, die außerhalb eines definierten Kreises an Personen eigentlich niemand sehen dürfte. Der laxen Umgang, wenn z.B. ausgetauschte Daten nicht sofort nach der Transaktion wieder gelöscht werden, vergrößert dieses Sicherheitsproblem. Auch für diese Art von Datenaustausch sollten verbindliche Regeln existieren, die zudem einer Überwachung unterliegen. Diese kann so gestaltet sein, dass zumindest die Schreib- und Leseaktionen aufgezeichnet werden. Damit lässt sich dann der Missbrauch nicht verhindern, aber zumindest im Nachhinein nachvollziehen.

Maßnahmen aus diesem Bereich sind nachfolgend aufgeführt:

- Erstellung einer Richtlinie, die für jede Art der Datenübertragung, abhängig vom Schutzbedarf der übertragenen Daten, die Methode vorgibt
- Sicherstellung, dass es für jede Art der Datenübertragung eine sichere technische Lösung gibt, die man den Mitarbeitern anbieten kann
- Information und Schulung der Mitarbeiter, wie sie bei der Datenübermittlung vorgehen müssen. Dazu gehört auch eine Unterweisung in den zu nutzenden Werkzeugen.



- Für den Transport von defekten IT-Systemen zur Reparaturstelle wie Arbeitsplatzrechnern, Servern, einzelnen Festplatten oder Druckern mit Festplatte, müssen sichere Transportmöglichkeiten vorhanden sein.
- Laptops, auf denen sensible Daten abgelegt sind, müssen verschlüsselt sein.

9.3.4 Eingabekontrolle

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.

Die Erfassung und Protokollierung, **wer wann welche** Eingaben getätigter hat, fällt unter den Oberbegriff der Eingabekontrolle. Ziel ist es, eine weitgehend revisionssichere Nachvollziehbarkeit eingegebener Daten sicherzustellen. Die Eingabekontrolle ist die Maßnahme, deren Einsatz am genauesten überprüft werden muss. Zum einen ist es nicht in jedem Fall technisch überhaupt möglich, alle Eingaben zu erfassen und zu protokollieren. In anderen Fällen ist es schlicht nicht erlaubt, es zu tun, oder der Aufwand übersteigt den Nutzen bei Weitem. Die Verhältnismäßigkeit von Aufwand und Nutzen zum einen und die Abwägung gesetzlicher Vorschriften wie die des Betriebsverfassungsgesetzes und der EU-DSGVO zum anderen muss genauestens geprüft werden.

Unter den Systemen, die eine Eingabekontrolle häufig bereits mitbringen, sind Personalsysteme und allgemein datenbankgestützte Umgebungen. In diesen Fällen wird kontrolliert,

- welcher Datensatz betroffen ist,
- welche Aktion angewendet wurde (Neuanlage, Veränderung oder Löschung),
- wer diese Aktion angestoßen hat und
- wann dies stattgefunden hat.

Die Neuanlage eines Datensatzes oder eines Dokuments zu erfassen, ist in den meisten IT-Systemen standardmäßig möglich. Änderungen werden aber schon häufig nur pauschal für das gesamte Dokument in Form von Änderer und Änderungsdatum festgehalten. Welche inhaltlichen Stellen davon betroffen waren, also die Änderungshistorie, wird häufig bereits nicht mehr erfasst.



Daraus wird ersichtlich, dass ein Änderungslog unabhängig von Datensätzen und Dokumenten existieren muss. Dieses wird bis zur Löschung des Datensatzes fortgeführt und kann auch danach noch Auskunft über jede Änderung geben.

9.3.5 Verfügbarkeitskontrolle, Wiederherstellbarkeit und Zuverlässigkeit

Verfügbarkeitskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

Wiederherstellbarkeit

9

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Zuverlässigkeit

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

Die Verfügbarkeitskontrolle und die im Bundesdatenschutzgesetz-Neu neu hinzugekommenen Kontrollen »Wiederherstellbarkeit« und »Zuverlässigkeit« fassen alle Maßnahmen zusammen, die der Sicherstellung der Verfügbarkeit von Daten dienen. Im Arbeitsfeld Business Continuity Management werden diese Maßnahmen im Rahmen des Verfügbarkeitsmanagements, der Notfallvorsorge und des IT-Notfallmanagements aufgeführt. Ein weiterer Aspekt ist die Wiederherstellung von IT-Systemen, Applikationen und Daten nach einem Systemverlust durch Faktoren wie Brand oder Sabotage. In den entsprechenden Kapiteln werden diese Themengebiete detaillierter ausgeführt.

Folgende Maßnahmen werden der Verfügbarkeitskontrolle und der Zuverlässigkeit zugeordnet:

■ Schutz vor Naturelementen und physischer Schutz

- Zutritt zu Daten verarbeitenden Systemen und damit auch Zugriff auf Daten. Maßnahmen aus dem Bereich Zutrittskontrolle finden hier Anwendung.
- Schutz vor Wasser, Feuer, Naturkatastrophen



- Schutz vor dem Angriff durch Dritte
 - Schutzmaßnahmen gegen Sabotage oder Cyber-Angriffe
- Sicherstellung der Verfügbarkeit der Infrastruktur
 - Maßnahmen aus dem IT-Notfallmanagement
 - Sichere und unterbrechungsfreie Stromversorgung (USV)
 - Klimatisierung
 - Überspannungsschutz
 - Einrichtung redundanter IT-Systeme, falls sinnvoll
- Bestandssicherung
 - Datensicherung/Wiederherstellung (Backup/Restore)
 - Vorsorge zur Rettung von versehentlich gelöschten oder veränderten Daten
 - Archivierung von Daten auf Grundlage von gesetzlichen und vertraglichen Erfordernissen
 - Notfalldatensicherung für den Fall einer Katastrophe
- Technisches IT-Security-Management
 - Virenschutzkonzept
 - Firewall-Konzept
 - Intrusion-Detection-System (IDS)
 - Patchmanagement
 - Verschlüsselung
 - Vertragsgestaltung
 - ...
- Notfallmanagement inklusive der Wiederherstellung der Verfügbarkeit von IT-Systemen, Applikationen und Daten

9.3.6 Datenintegrität

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

Die Integrität personenbezogener Daten ist neu in die Liste der Technisch-Organisatorischen Maßnahmen aufgenommen worden. Sie hat vor allem



zum Ziel, den Fokus bei der technischen Planung und Implementierung von Daten verarbeitenden Systemen verstärkt auf das Schutzziel »Integrität« zu richten. Damit steht dieses Schutzziel gleichberechtigt neben den Schutzzie- len Vertraulichkeit und Verfügbarkeit, was es dem IT-Security-Manager leichter macht, entsprechende Richtlinien zu erlassen und in der Praxis umzusetzen. Ebenso wie andere Maßnahmen auch macht es Sinn, diese Maßnahme schon im Vorfeld einer Implementierung zu betrachten und strategisch einzuplanen. Wenn man große Softwareprojekte betrachtet, dann fällt schnell auf, dass es neben der eigentlichen Software-Plattform zahlreiche Schnittstellen und untergeordnete Applikationen gibt und dass diese alle mitbetrachtet werden müssen.

9

9.4 Verschlüsselung

Das Verschlüsseln von Informationen ist eine sehr alte Technik und wurde bereits in der Antike genutzt. Sie schützt Informationen (in unserem Fall in Form von Daten) nicht vor Diebstahl, sondern davor, in ein sinnvolles, lesbbares Format gebracht zu werden. Nur die Verschlüsselungspartner, die jeweils die technische Möglichkeit haben, die Daten zu entschlüsseln, können mit den Daten und den darin enthaltenen Informationen etwas anfangen.

Hinweis

Verschlüsselung adressiert direkt das Schutzziel der Vertraulichkeit, also die Gewährleistung, dass Informationen nur von dem Personenkreis gelesen werden können, für den sie bestimmt sind. Sind die Daten verschlüsselt, dann ist es zudem fast unmöglich, gezielt Inhalte zu verändern. In diesem Fall wird auch das Schutzziel der »Integrität« erfüllt.

Dritte, die nicht über den erforderlichen Schlüssel zum Entschlüsseln der Daten verfügen, werden immer versuchen, durch die Nutzung mathematischer Algorithmen oder durch schieres Ausprobieren die Verschlüsselung zu knacken. Dieser Wettkampf führt dazu, dass sowohl die Techniken der Angreifer als auch die Methoden der Verteidiger technisch immer anspruchsvoller werden.



Mit dem technischen Fortschritt und der steigenden Leistungsfähigkeit von IT-Systemen, ganz zu schweigen von den kommenden Quantencomputern, müssen auch die Verschlüsselungsalgorithmen und Schlüssellängen laufend verbessert werden. Die großen, nationalen Sicherheitsbehörden veröffentlichen deshalb regelmäßig Papiere, die aufzeigen, welche Verschlüsselungstechniken noch sicher sind und welche nicht. Der Austausch alter Verschlüsselungssoftware gegen die jeweils aktuelle ist dabei eine Herausforderung, die die Unternehmen aber auch die Hersteller häufig nicht bewältigen können. Der Manager IT-Security hat dabei die zentrale Aufgabe, vorausschauend den Stand der Technik zu beobachten und rechtzeitig Anpassungen anzustoßen und konsequent zu verfolgen. Eine entsprechende Richtlinie, die die erlaubten Verschlüsselungstechniken aufführt, spielt dabei eine zentrale Rolle.

9.4.1 Begriffsbestimmungen

Die Wissenschaft der Verschlüsselung hat eine ganze Reihe von fachspezifischen Ausdrücken hervorgebracht, die zum großen Teil kaum durch Synonyme umschrieben werden können. Dies wäre auch nicht sinnvoll, da es die Kommunikation zwischen den Experten erschweren würde und im schlimmsten Fall zu Missdeutungen führen könnte.

Wichtige Begriffe aus der Verschlüsselungstechnik werden nachfolgend aufgeführt:

- Die **Verschlüsselung** ist eine Methode, **Klartext** in einen **Geheimtext** zu überführen. Die **Entschlüsselung** beschreibt den umgekehrten Vorgang, Geheimtext in Klartext zu übersetzen.
- **Kryptografie** ist die Lehre der Verschlüsselung und damit des Schutzes von Informationen durch Verschlüsseln.
- Bei der Verschlüsselungstechnik der **Chiffrierung** werden Texte anhand eines Verschlüsselungsverfahrens verschlüsselt. Ein Beispiel ist die Ersetzung jedes einzelnen Buchstabens durch einen definierten anderen. Nur wer weiß, wie dieser Vorgang wieder rückgängig gemacht werden kann, wird so an den ursprünglichen Klartext gelangen.
- Das **Kryptosystem** ist das System, das die Verschlüsselung und Entschlüsselung durchführt. Es enthält alle dafür erforderlichen Werkzeuge wie z.B. den Schlüssel und den verwendeten Algorithmus.



- Der **Pre-shared Key** (PSK) ist der vereinbarte Schlüssel, mit dem eine asymmetrische Verschlüsselung aufgebaut werden soll. Wie es der Name schon andeutet, wird der Schlüssel im Vorfeld ausgetauscht, damit beide Parteien Datenströme verschlüsseln und entschlüsseln können.
- Das **Public-Key-Verfahren** beruht auf der asymmetrischen Verschlüsselung und damit auf dem Vorhandensein von öffentlichen (*public*) und privaten (*private*) Schlüsseln.

9.4.2 Symmetrische Verschlüsselungssysteme

Das symmetrische Verschlüsselungsverfahren ist dadurch gekennzeichnet, dass sowohl die Partei, die die Verschlüsselung vornimmt, als auch der Gegenpart, der die Nachricht entschlüsseln möchte, denselben Schlüssel benutzt. In manchen Verfahren sind die Schlüssel allerdings nicht identisch, sondern müssen erst durch mathematische Algorithmen voneinander abgeleitet werden. Dies bleibt sich aber gleich, denn grundsätzlich muss der Schlüssel zunächst zwischen den beiden Parteien ausgetauscht werden, bevor der Zugriff auf den Klartext stattfinden kann.

Aus dem erforderlichen Austausch des Schlüssels ergeben sich einige Probleme. Erst muss ein sicherer Kommunikationskanal gefunden werden, der sicherstellt, dass die Übermittlung des Schlüssels nicht abgefangen werden kann, und zum anderen ist es erforderlich, genau zu dokumentieren, wer den Schlüssel für welche verschlüsselten Informationen besitzt.

Wichtig

Wird einer der Schlüsselträger selbst zu einem Sicherheitsrisiko, so muss eindeutig dokumentiert sein, welche Informationen gefährdet sind, und zudem müssen Prozesse installiert sein, die sicherstellen, dass die Daten unverzüglich mit neuen Parametern neu verschlüsselt werden.

Die Übertragung von symmetrischen Schlüsseln erfolgt heute oft per Telefon, z.B. wenn es um den Aufbau eines Standort-zu-Standort-VPNs geht und der Pre-shared Key ausgetauscht werden muss.

Die Sicherstellung, dass sich einmal ausgetauschte Schlüssel immer dort befinden, wo man es erwartet, ist ein schwieriges bis unmögliches Unterfan-



gen. Steigt die Anzahl der Partner, die über einen Schlüssel verfügen, so wird parallel zum steigenden Risiko des Missbrauchs automatisch auch der Aufwand immer größer, den Schlüssel zu ändern. Trotzdem werden überwiegend symmetrische Verfahren angewendet. Stand heute sind sehr viele technische Gerätschaften nicht in der Lage, ein anderes Verfahren zu unterstützen, und zwingen den Betreiber dazu, Pre-shared Keys zu nutzen. Ein weites Feld ist z.B. die Nutzung von Geräten in Wireless-Umgebungen. Industriell genutzte Barcode-Scanner nutzen in den meisten Fällen eine Verschlüsselung, die auf einem fest eingegebenen Schlüssel basiert. Für Arbeitsplatzrechner und Laptops ist es deutlich einfacher, andere, sicherere Methoden einzusetzen.

9.4.3 Asymmetrische Verschlüsselungsverfahren

Beim asymmetrischen Verschlüsselungsverfahren werden unterschiedliche Schlüssel zum Verschlüsseln und zum Entschlüsseln benutzt. Der sogenannte **öffentliche Schlüssel** des Empfängers dient dabei der Verschlüsselung und der **private Schlüssel** des Empfängers der Botschaft der Entschlüsselung.

Jede Partei verfügt über beide Arten von Schlüsseln. Wobei nur der öffentliche Schlüssel, das suggeriert bereits die Bezeichnung, an den Partner weitergegeben werden darf.

Neben der reinen Verschlüsselung kann das als Public Key bezeichnete Verfahren auch für die Erstellung von digitalen Signaturen, also die Sicherstellung von Authentizität und zur Authentifizierung genutzt werden. Der öffentliche Schlüssel wird in diesem Rahmen zur Verschlüsselung oder zur Überprüfung einer digitalen Signatur genutzt. Der private Schlüssel dient im Gegenzug zur Entschlüsselung oder zur Erzeugung von digitalen Signaturen.

Im Gegensatz zum symmetrischen Verfahren fällt die Problematik des sicheren Austauschs von Schlüsseln weitgehend weg. Der öffentliche Schlüssel kann ohne Ergreifung zusätzlicher Sicherheitsmaßnahmen, z.B. per E-Mail, ausgetauscht werden. Das bedeutet gleichzeitig, dass sich jede Partei nur darum kümmern muss, den eigenen privaten Schlüssel geheim zu halten. Der Verlust von eigenen oder fremden öffentlichen Schlüsseln ist zunächst unproblematisch.

Es ist trotzdem zu bedenken, dass derjenige, der die Verschlüsselung vornimmt, darauf vertrauen muss, dass der von ihm verwendete öffentliche Schlüssel auch wirklich von der Partei stammt, für die die Nachricht gedacht



ist. Daraus folgt, dass einiger Aufwand getätigt werden muss, genau dies sicherzustellen. Aus diesem Grund gibt es einige zentrale akkreditierte Zertifizierungsstellen, die diese Aufgabe wahrnehmen.

Da jede Nachricht mit dem öffentlichen Schlüssel der Gegenseite verschlüsselt werden muss, geschieht dies bei mehreren Empfängern derselben Nachricht auch mehrfach. Handelt es sich dabei um große Datenmengen, so kommen neben der Dauer, die ein solcher Vorgang in Anspruch nimmt, auch Probleme bei der Bandbreite hinzu. Aus einer Nachricht an 100 Empfänger werden dann, je nach zugrunde liegendem System, auch 100 unterschiedlich verschlüsselte Datenpakete, die einzeln über das LAN oder WAN übermittelt werden müssen. Das ist einer der Gründe, warum innerhalb von Unternehmensnetzwerken häufig auf diese sogenannte »Punkt-zu-Punkt-Verschlüsselung« verzichtet wird.

9

9.5 Cloud Computing

Bevor über die Sicherheit im Bereich des Cloud Computings gesprochen werden kann, ist es zunächst erforderlich, zu definieren, welche Teilbereiche Cloud Computing hat und welche wir davon nachfolgend betrachten werden. Ähnlich wie in anderen Fällen wird auch dieser Begriff für eine Vielzahl von Servicedienstleistungen genutzt, um diese, auch wenn sie bereits seit vielen Jahren angeboten werden, moderner klingen zu lassen. Besonders häufig wird das Outsourcing von IT-Infrastrukturen oder die Verlagerung von Datensicherungsprozessen an alternative, sichere Standorte als Cloud Computing bezeichnet.

Auf Basis eines vom National Institute of Standards and Technology, kurz NIST, veröffentlichten Whitepapers lassen sich die wesentlichen Charaktereigenschaften einer Cloud ableiten. So handelt es sich dann um Cloud Computing, wenn im Wesentlichen folgende Kriterien erfüllt sind:

- **Eigenständige, dynamische und skalierbare Nutzung (on-demand self service):** Der Nutzer kann bei Bedarf, möglichst ohne Interaktion mit Personal des Anbieters, eingekaufte Services wie CPU-Zeit oder Speicher anfordern und bekommt diese daraufhin umgehend zur Verfügung gestellt. In vielen Unternehmen decken die Leistungen der Cloud auch nur entstehende Engpässe ab, z.B. beim Auftreten von Bedarfsspitzen. Üblicherweise



se wird zu diesem Zweck ein Web-Formular genutzt, in dem mittels weniger Mausklicks der neue Bedarf eingestellt wird, oder aber der Zugriff erfolgt komplett automatisiert. Die dadurch entstehende Flexibilität ist eines der wichtigsten Charakteristiken des Cloud Computings und erfordert auf Seiten des Anbieters eine ausgeklügelte, häufig virtualisierte Umgebung.

- **Vielfältige Möglichkeiten des Netzwerzugangs (*broad network access*):** Die Verlagerung von Dienstleistungen in eine von Externen betriebene Infrastruktur darf nicht darin münden, dass IT-Angebote, die bisher schnell und zuverlässig funktioniert haben, auf einmal Einschränkungen unterworfen sind. Davon abgeleitet muss der Anbieter jede erforderliche Zugangsart zur Cloud anbieten. Neben dem reinen Zugriff spielt auch die Zugriffsgeschwindigkeit eine Rolle. Die wichtigen Parameter diesbezüglich sind die Latenz und der Durchsatz. Die Latenz beschreibt die Laufzeit von Datenpaketen im Netzwerk. Verlagert der Anbieter intern Server von Europa in die USA, dann wird die Latenz alleine schon aufgrund der längeren Kabellängen und zusätzlicher, zwischengeschalteter aktiver Netzwerkkomponenten höher werden. Neben der Latenz spielt die zur Verfügung stehende Bandbreite vom Endgerät zu den Daten oder Services in der Cloud eine wichtige Rolle. Sind die Daten zudem überregional verteilt abgelegt, dann können daraus durchaus stark variiierende Zugriffsgeschwindigkeiten resultieren.
- **Resource Pooling:** Um flexibler Nachfrage durch Nutzer der Cloud gerecht werden zu können, ist es nicht zweckmäßig, dedizierte Datenspeicher je Kunde bereitzuhalten. Das Wesen einer Cloud liegt darin, dass sich Nutzer einen großen Speicher- oder CPU-Pool teilen. Benötigt ein Nutzer weniger CPU-Zeit, dann kann diese von einem anderen Nutzer angefordert werden.

Die eben beschriebenen Parameter von Cloud-Lösungen lassen sich beliebig kombinieren. Aus diesen Kombinationen heraus haben sich vier Hauptkategorien an Cloud-Lösungen herausgebildet, die aktuell vermarktet werden. So unterscheidet man heute im Wesentlichen die folgenden Cloud-Kategorien:

- Public Clouds
- Private Clouds
- Hybrid Clouds und
- Community Clouds



Natürlich sind beliebige Mischformen denkbar, die sehr bald eigene Bezeichnungen erhalten werden.

Die Kategorie, die wir in den folgenden Kapiteln im Auge haben, sind die **Public Clouds**. Diese Form wird am häufigsten eingesetzt, da sie am ehesten dem wirtschaftlichen Bedürfnis nach »schnell, günstig und unkompliziert« folgt. Aus Sicht der IT-Security bringt sie allerdings auch die meisten Herausforderungen mit sich. Eine Public Cloud, hier ist auch des häufigeren der halb-deutsche Begriff »öffentliche Cloud« zu lesen, ist eine Dienstleistung eines Anbieters, des Cloud-Providers, die über das Internet frei zugänglich ist. Mit »frei zugänglich« ist in diesem Zusammenhang gemeint, dass zwischen dem Anbieter und dem Nutzer keine dedizierte, sichere (Stand-)Leitung, wie ein VPN, genutzt wird, sondern der Zugang von überall aus dem Internet möglich ist. Das minimiert mögliche Fehler, erhöht die Flexibilität und dadurch die Verfügbarkeit. Provider gibt es in der Regel für jede Art der Datenverarbeitung in großer Zahl. Das damit einhergehende Sicherheitsproblem ergibt sich daraus, dass der Nutzer der Public-Cloud-Lösung ab dem eigenen Internet-Zugang keine nachhaltige Kontrolle mehr über den Transport und die Verarbeitung der Daten hat. Dieses Risiko lässt sich über Vor-Ort-Audits etwas reduzieren, regelmäßig aber ist der Informationsgewinn bei der Besichtigung von Server-Racks und gut gereinigter Böden im Referenz-Rechenzentrum eher eingeschränkt. Hier helfen dann nur noch Zertifikate und in manchen Fällen Penetrationstests weiter.

Der Gegenpart der Public Cloud ist die **Private Cloud**. In diesem Fall verbleiben die Daten im Unternehmen. Dies kann dadurch gewährleistet werden, dass die gesamte Cloud-Infrastruktur im eigenen Rechenzentrum aufgebaut und betrieben wird. Es ist Software aus dem Open-Source-Bereich oder auch Standardsoftware von großen Anbietern verfügbar. Ein Vorteil ist dabei, dass definierte Daten auch für externe Partner zugänglich gemacht werden können. Damit schlägt man zwei Fliegen mit einer Klappe: Zum einen sind die datenschutzrelevanten oder auch sehr wichtigen Unternehmensdaten im eigenen Unternehmen gespeichert, zum anderen ist es dennoch möglich, den Datenaustausch mit Dritten kontrolliert und abgesichert zu gewährleisten. Der Grund, eine Private Cloud zu betreiben, beruht tatsächlich vorwiegend auf dem Schutzbedarf personenbezogener Daten. Den Nachweis zu führen, dass solcherart Daten in einer Public Cloud sicher verarbeitet werden, ist schon vom Grundgedanken her schwer. Datenflüsse, die man nicht kontrolliert, sind nicht verlässlich transparent darzustellen und Maßnahmen, die



davon abgeleitet werden, sind demzufolge schwer messbar. Eine Risikofolgeabschätzung, die bei sensiblen personenbezogenen Daten gesetzlich vorgeschrieben ist, ist damit fast unmöglich.

Die oben beschriebenen Nachteile einer Public Cloud haben in den letzten Jahren dazu geführt, dass viele Cloud-Anbieter eine Mischform zur Verfügung stellen, die die Vorteile einer Public Cloud nutzt, auf der anderen Seite aber den Schutz von Daten mit einem hohen Schutzbedarf sicherstellt. Die sogenannten **Hybrid Clouds** basieren darauf, dass die Dienstleistungen eines Anbieters im Internet genutzt werden können, während z.B. personenbezogene Daten oder kritische Daten im Unternehmensnetzwerk verbleiben. Dieser Spagat kann z.B. erreicht werden, indem Daten vor der Verarbeitung und vor dem Transfer zum Anbieter pseudonymisiert werden und dieser Vorgang nach der Verarbeitung, wenn die Ergebnisse wieder im Unternehmensnetzwerk sind, rückgängig gemacht werden. Das ist eine typische Nutzung der mit der EU-DSGVO neu eingeführten Pseudonymisierung von Daten. Mit der in der vorhergehenden Datenschutzbestimmung festgeschriebenen Anonymisierung der Daten wäre eine solche sichere Datenverarbeitung nicht möglich gewesen.

Die letzte Kategorie an Cloud, die ich vorstellen möchte, wohl wissend, dass sich diese Liste beliebig weiterführen lassen könnte, ist die **Community Cloud**. Hierbei handelt es sich um eine über verschiedene Unternehmen hinweg gemeinsam genutzte cloudbasierte Infrastruktur. Ein Beispiel wäre der Aufbau einer Community Cloud im Rahmen eines großen Bauprojekts. Mehrere Firmen können die Dienste nutzen, z.B. für Berechnungen oder Kostenkalkulationen. Dieses Beispiel zeigt schon den Unterschied zu einer Public Cloud. Bei einer Community Cloud ist der Nutzerkreis definiert und zumeist allen Teilnehmern bekannt. Aus Sicht der IT-Security können solche Clouds im Normalfall durch weitere Mechanismen z.B. den Zugriff auf die vorab festgelegten IP-Adressen der Teilnehmer beschränken.

Ein paar grundsätzliche Fakten gelten für jede der eben beschriebenen Kategorien des Cloud Computings und sollten Entscheidern bewusst sein, bevor sie sich für eine Art der Auslagerung und für einen bestimmten Anbieter entscheiden:

- Um die Aspekte der IT-Security hinsichtlich der Cloud beachten zu können, ist es erforderlich, bereits über ein funktionierendes IT-Security Management zu verfügen. Die Einbindung der Dienstleistungen in der Cloud



- in einen existierenden IT-Security-Regelkreis ist möglich, der Neuaufbau gezielt für diesen Zweck hingegen eher als schwierig einzuschätzen.
- Mit der Komplexität, die eine Auslagerung in die Cloud zwangsläufig mit sich bringt, steigen die Bedrohungen und damit auch das Risiko. Mit dem Risiko steigen die erforderlichen Maßnahmen, der Aufwand für deren Nachverfolgung wächst ebenso und schlussendlich auch die damit verbundenen Kosten. Diese Kosten sollten gegen die zu erwartenden Einsparungen gerechnet werden.
 - Mit der Abgabe von Daten an eine schwer örtlich und technisch lokalisierbare Cloud sinkt zwangsläufig die Transparenz dahin gehend, wo sich die eigenen Daten befinden und in welchem Status sich die IT-Security diesbezüglich befindet. Alle Angaben dazu stammen vom Anbieter selbst und damit aus zweiter Hand.
 - Wird die Speicherung von Daten nicht vertraglich so bestimmt, dass diese ausschließlich im Inland, bzw. in Europa, erfolgt, so müssen die juristischen Folgen im Einzelnen betrachtet werden.
 - Regelmäßige Audits von Daten verarbeitenden Systemen, die sich in der Cloud befinden, ist schwerlich möglich. In der EU-DSGVO wird im Grundsatz die Möglichkeit erwähnt, die Verarbeitung personenbezogener Daten zertifizieren zu lassen. Inwieweit dies in akzeptierten Prüfsiegeln für Cloud-Anbieter münden wird, ist aktuell nicht absehbar. Selbst durchgeführte Audits gestalten sich schwer, wenn der Cloud-Anbieter seine Rechenzentren über Kontinente verteilt aufstellt. Erheblich erschwert wird dies weiter, wenn der Provider selbst wieder über weitere Sublieferanten verfügt, an die er Teilaufgaben delegiert.
 - Mit der Auslagerung von Daten hin zu einem Anbieter entzieht man den eigenen Administratoren die Möglichkeit, Zugriffsprotokolle zu erstellen, und übergibt diese Aufgabe fremden Administratoren, die für den Anbieter arbeiten. Es ist schwer einzuschätzen, wie die Aussagekraft dieser Protokolle einzuschätzen ist.

9.5.1 Dienstleistungen in der Cloud

Im Großen und Ganzen unterscheidet man beim Cloud Computing zwischen vier verschiedenen Arten an Dienstleistungen. Jeder dieser Services kann einer Schicht im TCP/IP-OSI-Modell zugeordnet werden. Demzufolge wer-



den je nach Schicht im Zuge des IT-Security-Managements entsprechende Sicherheitskonzepte abgeleitet.

- **Software-as-a-Service (SaaS):** Die Spielart, Applikationen nicht auf eigenen Servern zu installieren, sondern in der Cloud zu betreiben, existiert mit am längsten. Aufgekommen ist der Bedarf nach diesen Lösungen mit der zunehmenden Komplexität von Softwareinstallationen und dem damit verbundenen Wartungsaufwand. Bei SaaS übernimmt der Anbieter die Installation, Fehlerbereinigung und Wartung der Software und bietet die Nutzung über eine Schnittstelle an. Der Kunde kann dabei flexibel über eine breit skalierbare Anzahl an gleichzeitig genutzten Installationen verfügen. Das ist vor allem dann sinnvoll, wenn z.B. aus saisonalen Gründen die Anzahl der Benutzer stark schwankt. Zusätzlich zum reinen Betrieb werden häufig auch Anpassungen vom Anbieter durchgeführt, die dann innerhalb kürzester Zeit allen Anwendern zur Verfügung stehen. Grundsätzlich können die Daten, die mit der angebotenen Anwendung verarbeitet werden, entweder lokal abgelegt sein, also innerhalb des eigenen Unternehmens, oder aber auch dezentral, also beim Cloud-Anbieter. Befinden sie sich beim Anbieter, dann sprechen wir gleichzeitig von »Storage-as-a-Service«.
- **Storage-as-a-Service:** Der Gedanke ist verlockend: Ein Unternehmen mit vielen Standorten auf der ganzen Welt legt seine Daten bei einem international agierenden Cloud-Provider ab, und jeder Mitarbeiter kann von jedem Ort auf die Daten zugreifen, für die er berechtigt wurde. In diesem Fall können Daten so genutzt werden, als wären sie auf eigenen Datenservern gespeichert, es können Daten archiviert werden oder aber es werden Daten in die Cloud gespiegelt und dienen als flexibel zugreifbare Datensicherung. Die entstehenden Sicherheitsprobleme, wenn ein Unternehmen seine Daten in dieser Form physisch aus der Hand gibt, werden in den nächsten Kapiteln beschrieben.
- **Platform-as-a-Service (PaaS):** Ähnlich wie bei Software-as-a-Service wird in diesem Fall eine Anwendung in der Cloud bereitgestellt. Der Unterschied liegt in der Komplexität. Handelt es sich bei SaaS eher um einzelne Applikationen wie eine Textverarbeitung oder ein Programm zur Fuhrparkverwaltung, so geht es bei PaaS schon eher um ein komplettes Produktionsystem. Neben der Komplexität der Anwendung und den damit einhergehenden Herausforderungen an die Konfiguration steigt in diesem Fall auch die Anzahl an angebundenen Systemen und damit die Schnittstellen überproportional.



Dieser Bereich wächst aktuell am schnellsten. Dienstleistungen wie Microsoft Office 365 in der Cloud werden dabei mit vielen weiteren Services des Anbieters gekoppelt, und um alle diese Leistungen nutzen zu können, wird es auch erforderlich sein, die zugehörigen Daten in der Cloud zu speichern.

- **Infrastructure-as-a-Service (IaaS):** Neben Daten und Applikationen lassen sich auch komplette Systeme in die Cloud verlagern. Darunter versteht man z.B. die Auslagerung einer Virtualisierungsumgebung. Werden neue Server benötigt, dann werden diese auf Knopfdruck eingerichtet und stehen umgehend zur Verfügung. Anhängige Dienstleistungen wie die Datensicherung, die Datenspeicherung und die Netzwerkanbindung lassen sich in solchen Angeboten hoch automatisiert mitbuchen. Der Vorteil liegt darin, dass keine eigene Hardware mehr benötigt wird und damit Abschreibungen auf Hardware und Platzbedarf für die physischen Komponenten wegfallen. Änderungen in den Anforderungen lassen sich schnell umsetzen und dies zu vertraglich festgelegten und damit kalkulierbaren Kosten.

Auch hier gilt, dass die Grenzen zwischen den verschiedenen Schichten und damit Dienstleistungen verschwimmen. Ein Anbieter von Speicherplatz, der zusätzlich eine Textverarbeitung und ein Datenbankprogramm für den Büroarbeiter anbietet und dazu eine Suchmaschine über alle in der Cloud abgelegten Dokumente, bietet auf einen Schlag mehrere Arten an Cloud-Diensten an. Vom Zugriff über den Browser auf dem Arbeitsplatzrechner auf die Anwendung in der Cloud, über die Möglichkeit, die Daten dort auch zu speichern und zu teilen, bis hin zu Dienstleistungen, die auf den gespeicherten Daten aufsetzen. Das bedeutet aber gleichzeitig, dass man den vollen Mehrwert an Funktionen nur dann nutzen kann, wenn man alle diese Dienste auch bei diesem einen Betreiber nutzt. Auf diese Weise entstehen wieder große Service-Anbieter und man entfernt sich wieder von der großen Vielfalt kleiner Anbieter, die noch vor Kurzem den Charme von Cloud Computing ausgemacht haben.

9.5.2 Risikofaktoren

Die Verlagerung von Dienstleistungen oder Daten in die Cloud hat neben gravierenden Anpassungen an Prozessen oder auch der Infrastruktur eines Unternehmens auch Folgen für die Informationssicherheit. Hier stellt sich



die Frage, inwieweit sich die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen lassen, wenn sich die zu schützenden Daten außerhalb des eigenen Zugriffsbereichs befinden. Damit kommen wir zu einem wesentlichen Aspekt der Cloud: die Virtualisierung. Im Falle der Public Clouds werden die Dienstleistungen in einer Form bereitgestellt, die es dem Anwender nicht ermöglicht, zu lokalisieren, auf welchem System oder an welchem Ort die Verarbeitung stattfindet. Handelt es sich um einen der großen Cloud-Anbieter, dann ist häufig nicht einmal das Land oder der Kontinent zu verorten, in dem die Infrastruktur steht, die den Cloud-Service anbietet. Dazu kommt, dass Cloud-Anbieter im Regelfall nicht alle Dienstleistungen selbst abdecken, sondern in den meisten Fällen über ein Netzwerk von eigenen Dienstleistern verfügen. Wird der Dienst Storage-as-a-Service genutzt, so können sich die primären Daten in einem komplett anderen Netz befinden als die Daten der Datensicherung. Werden Leistungsgrenzen des Anbieters überschritten, dann wird dieser sich wiederum so absichern, indem er Teile der Daten an Unterlieferanten auslagert. Die Flexibilität, die das Cloud Computing charakterisiert, wird in diesem Fall zum Bumerang, was die Berechenbarkeit des Sicherheitslevels angeht.

Neben den kritischen Fragen des Datenschutzes, die sich aus der Unfähigkeit ergeben, Daten und Dienstleistungen zu lokalisieren, sind viele technische Aspekte zu beachten. Insbesondere die angebotenen Leistungen müssen im Vorfeld besprochen und durch Service Level Agreements abgesichert werden.

Eine gute Quelle bezüglich der Vorgaben, die ein Cloud-Provider befolgen muss, ist die ISO-Norm 27018. Sie bezieht sich im Kern auf personenbezogene Daten, kann aber im Grunde für jede Art von ausgelagerter Datenverarbeitung herangezogen werden. Sie mappt alle Vorgaben auf die Kapitel der ISO 27002 und kann daher nahtlos im Rahmen des Aufbaus eines ISMS genutzt werden. In Anhang A werden Maßnahmen aufgeführt, die als Zusatz zu den Maßnahmen in Anhang A der ISO 27001 gesehen werden müssen.

Noch ergiebiger als die ISO-27018-Norm ist der Anforderungskatalog Cloud Computing des BSI, bekannt als »C5« des BSI. Er richtet sich an Cloud-Provider und listet dediziert Anforderungen auf. Wenn man als IT-Security-Verantwortlicher diese Anforderungen als eigene Anforderungen versteht, kann man daraus einen Prüfkatalog erstellen und diesen als Grundlage für eigene Audits nutzen.



Die folgende Tabelle beschäftigt sich mit dem Schutzziel **Vertraulichkeit** bezüglich des Cloud Computings und führt generische Fragen auf, die ein Cloud-Provider beantworten müssen:

Fragestellung	Beschreibung
Ist der Cloud-Anbieter nach BSI zertifiziert?	Ist der Anbieter nach BSI Cloud-zertifiziert, dann kann der Auftraggeber davon ausgehen, dass die grundlegenden Sicherheitsmaßnahmen ergriffen werden.
Werden die eigenen Daten und Dienstleistungen ausreichend sicher von denen anderer Kunden getrennt?	Ein Cloud-Anbieter hat naturgemäß viele Kunden, von denen einige auch als Konkurrenten auf dem Markt auftreten. Die Daten dieser Konkurrenten werden unter Umständen von einem Anbieter gesichert. Deshalb stellt sich die Frage, welche Maßnahmen der Anbieter implementiert hat, um den Durchgriff auf fremde Daten zu verhindern.
Ist der Zugang zu den Daten sicher?	Ausgelagerte Daten oder gar eine extern betriebene Systemlandschaft erfordern Mechanismen, um transparent und einfach aus dem Unternehmen heraus darauf zugreifen zu können. Transparenz und Einfachheit sind dabei die Anforderungen der Endkunden, absolute Sicherheit die der IT-Security-Organisation. Die Ende-zu-Ende-Verschlüsselung ist eine Maßnahme, um dies zu erreichen.
Ist der Zugang zur Administrationsseite ausreichend geschützt?	Neben dem Zugriff auf die Daten ist auch der Zugriff auf die Administrationswerkzeuge ein kritischer Punkt. Erfolgt hier die Authentifizierung nicht durch sichere Mechanismen und können Unbefugte hierauf zugreifen, dann ist die Sicherheit der gesamten Struktur infrage gestellt.
Können die Daten, die beim Cloud-Anbieter liegen, verschlüsselt werden?	Nur durch die selbst durchgeführte Verschlüsselung von Daten kann der Missbrauch durch den Provider verhindert werden. Verlässt man sich auf die Verschlüsselung durch den Provider, ist man als Unternehmen auf die Integrität der Administratoren beim Anbieter angewiesen. Da die Verschlüsselung die Komplexität stark erhöht und den einfachen Zugriff erschwert, dreht sich die Diskussion häufig darum, einen Kompromiss zu finden. Im Falle von sensiblen bzw. personenbezogenen Daten darf dieser allerdings nicht auf Kosten der Datensicherheit gehen.



Fragestellung	Beschreibung
Können die Daten zum Cloud-Anbieter verschlüsselt übertragen werden? Welche Art von Verschlüsselung ist in Benutzung?	Die Speicherung von Daten beim Cloud-Anbieter in verschlüsselter Form ist die eine Erforderlichkeit. Die andere ist die verschlüsselte Übertragung der Daten zum Provider. Ob dies bereits ab dem Arbeitsplatz des Endanwenders geschehen muss oder erst dann, wenn die Daten die Unternehmens-Firewall verlassen, hängt von der Risikobewertung ab.
Können die Daten, die beim Provider liegen, durch einen Schlüssel verschlüsselt werden, auf den nur der Auftraggeber Zugriff hat?	Das »Bring Your Own Key« (BYOK) genannte Verfahren basiert darauf, dass möglichst in der Public-Key-Infrastruktur (PKI) des Auftraggebers ein asymmetrisches Schlüsselpaar erzeugt wird, mit dem die Verschlüsselung der Daten beim Cloud-Anbieter erfolgt. Das bedeutet zum einen, dass der Cloud-Anbieter keinen Zugriff auf die verschlüsselten Daten hat mit dem Nachteil, dass dieser deshalb auch keine weiteren Dienste einsetzen kann, wie das Durchsuchen des Datenbestands.
Können eigene Sicherheitsprodukte und Methoden auch dann genutzt werden, wenn Daten oder sogar Teile der IT-Infrastruktur beim Cloud-Anbieter liegen?	Antivirus, Audit-Werkzeuge, Monitoring oder Zugriffsprotokollierung sind Sicherheitswerkzeuge. Werden diese innerhalb des Unternehmens eingesetzt, so gibt es keinen Grund, dies nicht auch auf die in die Cloud ausgelagerten Daten auszudehnen. Oft stellen die Anbieter entsprechende Werkzeuge zur Verfügung. Ob diese ausreichend sind, muss individuell entschieden werden.
Wird beim Cloud-Anbieter eine sichere virtuelle Umgebung angeboten?	Ein Beispiel, bei dem sehr häufig Virtualisierung genutzt wird, ist das Serverhosting. Auf einem Hostsystem werden dabei weitere Gastsysteme eingerichtet. Das Risiko liegt vor allem in zwei Bedrohungen begründet: Zum einen kann es theoretisch möglich sein, von Gastsystem zu Gastsystem überzugreifen, und zum anderen kann das Hostsystem komrompitiert werden und dann auf die Gastsysteme zugegriffen werden.



Fragestellung	Beschreibung
Wie sehen die Maßnahmen zur Abwehr von Angriffen von innen (von Mitarbeitern des Anbieters) und von außen (über das Internet) aus?	Cloud-Anbieter stehen weit mehr im Fokus von potenziellen Angreifern als die allermeisten Unternehmen. Das liegt naturgemäß vor allem darin begründet, dass dort auf einen Schlag Daten vieler Firmen zu erbeuten wären. Deshalb ist es auch nicht verwunderlich, dass es bereits heute Informationen über geglückte Angriffe auf große Cloud-Anbieter gibt. Diesen Angriffen präventiv zu begegnen, ist eine grundlegende Aufgabe der Cloud-Betreiber. Dazu gehört natürlich auch ein ausgereiftes und vollständiges IT-Security-Management.
Sind alle datenschutzrelevanten Punkte geklärt?	Werden personenbezogene Daten in der Cloud gespeichert oder durch die Cloud zugegriffen, so gelten die Bestimmungen der EU-DSGVO und des Bundesdatenschutzgesetzes-Neu.
Wird die Sicherheitslage regelmäßig durch externe Experten geprüft?	Die Auditierung der Infrastruktur des Cloud-Anbieters und aller anderen Dienstleister ist die Grundlage für die Erfüllung der Anforderungen aus Sicht der IT-Security. Die Auditierung sollte von einer unabhängigen Stelle aus durchgeführt werden und muss von der Qualität den höchsten Ansprüchen genügen. Die Ergebnisse und der Fortschritt der Abarbeitung müssen transparent dargestellt werden. Steht am Ende die Erteilung eines Prüfsiegels, dann ist dieses zu prüfen.

Anforderungen an die **Verfügbarkeit** von Dienstleistungen aus der Cloud stellen sich vom ersten Tag der Anbindung an und werden in der folgenden Tabelle gegliedert:

Fragestellung	Beschreibung
Können die Dienstleistungen in der gewünschten Geschwindigkeit geleistet werden?	Die Frage der Qualität von Cloud-Services spielt eine maßgebliche Rolle. Dabei muss beachtet werden, dass jede Stelle, die auf die Dienstleistung zugreifen möchte, mit in die Qualitätsüberwachung aufgenommen werden muss. Es nützt den Kollegen in Südafrika nicht viel, wenn die Daten, die letztendlich in Irland abgelegt sind, aus Frankreich ausreichend schnell im Zugriff sind, von Südafrika aus aber nicht.



Fragestellung	Beschreibung
Können die Dienstleistungen mit der gewünschten Verfügbarkeit bereitgestellt werden?	Bei Cloud-Services hängt die Verfügbarkeit in hohem Maße von Stellen ab, die das eigene Unternehmen selbst kaum technisch beeinflussen kann. Neben dem Cloud-Provider selbst handelt es sich dabei vor allem um zwischengeschaltete Netzwerkbetreiber und deren Lieferanten. So kann bereits ein langsamer Internet-Zugriff in einem Standort den weltweiten Einsatz einer Cloud-Lösung behindern. Entscheidet sich ein Unternehmen generell dazu, Clouds zu nutzen, dann hat dies immer auch Einfluss auf die eigene Infrastrukturarchitektur, insbesondere die Anbindung an das Internet.
Werden Daten und Konfigurationen gesichert?	Die Datensicherung ist ein entscheidendes Thema für alle Daten, die sich in der Cloud befinden. Die Kriterien müssen so gewählt werden, dass alle möglichen Notfallszenarien dadurch abgedeckt werden. Im Rahmen des Schutzzieles Belastbarkeit ist die Datensicherung von besonderem Interesse. Je nach Art der verarbeiteten Daten sollte ein Dienstleister gewählt werden, der die Daten verarbeitenden Systeme physisch getrennt redundant implementiert hat.
Ist ein adäquates IT-Notfallmanagement installiert?	Probleme können jederzeit auftreten, und wird ein Unternehmen dadurch von den eingekauften Cloud-Services abgeschnitten, dann werden sie sehr schnell zu einer Krise. Neben Datensicherungsmaßnahmen zählen auch redundante Anbindungen und redundante Infrastrukturen zu den ersten Maßnahmen. Dazu kommen alle Mechanismen des IT-Notfallmanagements wie die Alarmierung etc.
Werden die Systeme des Cloud-Providers und alle weiteren erforderlichen IT-Systeme und Netze von Unterlieferanten ausreichend gewartet?	Der Weg vom Arbeitsplatz bis zu den Daten oder Dienstleistungen des Cloud-Providers ist lang und wird durch unterschiedliche Anbieter betreut. Alle Systeme, die für den Betrieb erforderlich sind, müssen stets auf einem aktuellen Stand sein. Das betrifft neben der reinen Konfiguration auch das Firmware-, Fehler- und Patchmanagement.

Die letzte Tabelle beschäftigt sich mit der Frage der **Qualität** der Bereitstellung von Daten aus der Cloud:



Fragestellung	Beschreibung
Können die Dienstleistungen in der gewünschten Qualität geliefert werden?	Der Verlust von Daten oder die ungewollte Änderung von Dateninhalten ist ein Sachverhalt, der verhindert werden muss. Dies kann durch den Einsatz von Checksummen oder die kontinuierliche Überprüfung der Daten geschehen. Dazu kommen Mechanismen der Transaktion, die verhindern sollen, dass Datenabbrüche während der Eingabe oder Übermittlung zu fragmentierten und inkonsistenten Datenbeständen führen.
Ist die Dienstleistung flexibel genug, auf die Bedürfnisse des Auftraggebers einzugehen?	Ein Grund, warum Public-Cloud-Services im Vergleich günstig sind, liegt in der Standardisierung des Angebots. Je stringenter das Standardangebot ist, desto unflexibler wird der Anbieter auf Änderungswünsche reagieren.

9

Neben technischen Aspekten, den Punkten der IT-Security und den Anforderungen aus Sicht des Datenschutzes definieren noch weitere Stellen im Unternehmen Vorgaben, was die Speicherung und Verarbeitung von Daten betrifft. Betroffen sind vor allem auch alle Stellen im Unternehmen, die steuerlich relevante Daten ablegen müssen. In diesem Fall besteht z.B. die gesetzliche Anforderung, dass alle Daten im Inland abzulegen sind. Auf Antrag kann dies zwar auf alle Mitgliedsstaaten der Europäischen Union ausgedehnt werden, diejenigen Länder wie die USA, die am meisten Cloud-Dienste anbieten, sind davon aber ausgenommen. Eine ähnliche Regelung gibt es nach Handelsrecht auch für Buchungsbelege und Handelsbriefe. In allen Fällen müssen auch die Aufbewahrungsfristen beachtet werden, und der Zugriff durch staatliche Stellen muss technisch gewährleistet sein.

Hinweis

Jeder einzelne Cloud-Service ist Teil einer übergeordneten Servicearchitektur im Unternehmen. Immer häufiger werden immer kleiner werdende Teilprozesse in Form von Cloud-Dienstleistungen ausgelagert. Das führt dann schnell dazu, dass z.B. Auswertungen und Reports, die eine ganze Reihe von Eingabedaten benötigen, nicht mehr ohne Weiteres erstellt werden können, da die Grunddaten auf verschiedene Anbieter verteilt sind. Komplexe Mechanismen wie z.B. die Korruptionsbekämp-



fung können dadurch ausgebremst werden. Solche Prozesse korrelieren verschiedenste Daten, um Missbrauch festzustellen. Sind diese Daten aber nicht direkt erreichbar, dann ist auch keine Auswertung möglich. Dieses Problem kommt auch im Bereich der Big-Data-Verarbeitung zum Tragen.

9.5.3 Datenschutzrechtliche Aspekte

Die EU-DSGVO treibt die EU-weite Harmonisierung des Datenschutzes voran. Heute achten die meisten deutschen Unternehmen noch darauf, dass ein Public-Cloud-Anbieter die Daten in einem deutschen Rechenzentrum verarbeitet. Dies wird sich mittelfristig ändern und dann wird es aus Sicht des Datenschutzes weniger wichtig sein, in welchem europäischen Land das Rechenzentrum steht. Ein wichtiges Prinzip, das die EU-DSGVO mit sich bringt, ist das »Marktortprinzip«. Es soll sicherstellen, dass diese Verordnung auch von Anbietern aus Drittstaaten einzuhalten ist, wenn personenbezogene Daten von europäischen Bürgern verarbeitet werden. Ein Marktvorteil für Deutschland ist das Bundesdatenschutzgesetz-Neu, das in Europa mit zu den strengsten gehört, und damit ist die Nutzung eines deutschen Rechenzentrums weiterhin von Vorteil.

Cloud Computing fällt in den Bereich der klassischen Auftragsverarbeitung. Wie bisher auch regelt die EU-DSGVO, dass der Auftraggeber der Cloud-Dienstleistung für den Datenschutz verantwortlich bleibt, auch wenn sich seine Daten in einer Cloud befinden. Auftraggeber sollen laut EU-DSGVO nur solche Cloud-Anbieter beauftragen, »die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der EU-DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet«. Daraus folgt, dass der Auftraggeber bei der Vertragsgestaltung darauf achten muss, dass die von der EU-DSGVO aufgeführten Vorgaben erfüllt werden. Des Weiteren muss er die Umsetzung prüfen. Das Gesetz sieht explizit vor, dass die »Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens durch einen Auftragsverarbeiter als Faktor herangezogen werden kann«, um hinreichende Garantien für den Datenschutz und die Datensicherheit in der Public Cloud nach EU-DSGVO-Vorgaben nachzuweisen. Hier ist die Formulierung »als Faktor« zu



beachten. Eine Zertifizierung entlässt den Auftraggeber nicht aus seiner Verantwortung, sie stellt aber ein gutes Werkzeug dar, einen Betreiber einzuschätzen. Bis die ersten anerkannten Prüfsiegel vergeben werden, kann allerdings noch einige Zeit vergehen.

Die stark erhöhten Bußgelder, die die EU-DSGVO vorsieht, erstrecken sich auch auf Verstöße im Zusammenhang mit der Nutzung von Clouds. Es ist also darauf zu achten, dass ein definierter Prozess zur Freigabe und Überprüfung von Cloud-Dienstleistungen verbindlich ist und dass alle genutzten Cloud-Dienstleistungen diesen durchlaufen.

Cloud Computing bedeutet Skalierbarkeit und wird demnach technisch zu meist nicht lokalisierbar sein. Das Datenschutzrecht dagegen ist eng verbunden mit dem Ort der Verarbeitung. Innerhalb des europäischen Binnenmarkts wird vorausgesetzt, dass ein vergleichbares Sicherheitsniveau bezüglich des Datenschutzes besteht, und damit existieren Möglichkeiten, durch entsprechende Verträge die Verarbeitung durch Dritte rechtlich abzusichern. Die EU-DSGVO wird diese Entwicklung weiter befördern, aber damit auch die Abgrenzung zu allen nicht-europäischen Ländern trennschräfer darstellen.

9

Hinweis

Auf die Anforderungen des Datenschutzes und weiterer lokaler Gesetzesvorschriften haben einige große Cloud-Anbieter reagiert und bieten an, Daten ausschließlich in europäischen Rechenzentren abzulegen und dies vertraglich zuzusichern.

Folgende Gesichtspunkte sollte man beachten, wenn man personenbezogene Daten in die Public Cloud auslagern will:

- Die Festlegung der verantwortlichen Stelle ist der Ausgangspunkt für die Überlassung von Daten an den Cloud-Betreiber. Darunter sind diejenigen Stellen zu sehen, die auf Seiten der Nutzer bestimmen, welche Daten unter welchen Voraussetzungen übertragen werden. Zur Beurteilung, ob dies im Einzelfall nach DSGVO und Bundesdatenschutzgesetz-Neu zulässig ist, muss der Datenschutzbeauftragte hinzugezogen werden.
- Ähnlich wie der bisherige Vertrag nach Bundesdatenschutzgesetz § 11 (ADV) muss ein Auftragsverarbeitungs-Vertrag (AV-Vertrag) nach Art. 28



EU-DSGVO mit dem Cloud-Betreiber abgeschlossen werden. Grundsätzlich steigen die Anforderungen an einen solchen Vertrag, auch wenn die Anzahl der Kriterien im Vergleich mit BDSG § 11 abgenommen haben. Das Verhältnis zwischen Auftraggeber und Auftragnehmer wird, vor allem was die Haftung angeht, nach EU-DSGVO auf eine höhere Stufe gestellt.

- Wie bisher auch muss der Anbieter überprüft werden. Als Rahmen können die Technisch-Organisatorischen Maßnahmen aus § 64 Bundesdatenschutzgesetz-Neu genutzt werden. Dafür muss der Auftraggeber aber alle Stellen kennen, die eine Verarbeitung der Daten vornehmen. An dieser Stelle wird deutlich, dass dies faktisch kaum möglich ist und sich der Nutzer auf entsprechende externe Prüfergebnisse und Zusicherungen des Dienstleisters verlassen muss. Prüfberichte von anerkannten externen Prüfern sollten dazu eingefordert werden. Außerdem sollte verlangt werden, dass der Zugriff auf diese Berichte und alle Protokolldateien ermöglicht wird. Daneben sollte man vom Betreiber verlangen, dass konkret aufgezeigt wird, welche Stellen an der Verarbeitung der Daten beteiligt sind. Dies umfasst auch alle Unterlieferanten.
- Durch Verträge mit dem Cloud-Betreiber sollte die Haftungsfrage geklärt sein.
- Der Cloud-Betreiber muss zustimmen, dass ein Datenschutz-Audit technisch und organisatorisch uneingeschränkt möglich ist.
- Die Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörden nach EU-DSGVO ist ein wichtiger Bestandteil der neuen Verordnung und die Abläufe, die einen solchen Vorgang ermöglichen, müssen dementsprechend ausgestaltet und dokumentiert sein.
- Müssen Daten gelöscht werden oder erfolgt ein Übergang von Daten von einem Lieferanten auf einen anderen, so muss dieses Prozedere von vornherein geregelt sein.

9.5.4 Vertragliche Vereinbarungen

Der Cloud-Vertrag regelt die Beziehungen zwischen Auftraggeber und Cloud-Anbieter und nimmt aus diesem Grund eine sehr wichtige Stellung ein. Dabei weichen die Inhalte kaum von denen eines Outsourcing-Vertrags ab.



Ein Cloud-Vertrag deckt zumindest die vier folgenden Themenbereiche ab:

- **Leistungsbeschreibung:** Ausgehend von einer Bedarfsanalyse beschreiben Leistungsscheine detailliert, welche Anforderungen der Kunde an den Cloud-Anbieter hat und wie und in welcher Geschwindigkeit er diese zu erfüllen hat. Gekoppelt an die Leistungsscheine sind die Service Level Agreements (SLAs) und die Sanktionen, die in Kraft treten, falls der Anbieter die vereinbarten Leistungen nicht erbringt.
- **Datenschutz:** Der Auftraggeber ist in der Verantwortung, die Belange des Datenschutzes in den Cloud-Vertrag zu tragen, falls personenbezogene Daten dort verarbeitet werden sollen.
- **IT-Security:** Wie sind die Daten geschützt und inwieweit kann dies durch den IT-Security-Verantwortlichen aufseiten des Auftraggebers überprüft werden?
- **Vertragsende:** Soll der Dienstleister gewechselt werden oder ein zusätzlicher Dienstleister Teilbereiche der Leistungen übernehmen, so muss dieser Übergang von vornherein geregelt sein. Stichpunkte sind hier das Löschen und die sichere Übertragung von Daten.

9

9.5.5 Sinnvolle Freigabeprozesse

In den letzten Abschnitten wurde über die verschiedenen Personengruppen berichtet, die innerhalb eines Freigabeprozesses zur Nutzung von Cloud-Lösungen ein Mitspracherecht haben. Angesichts der immer häufiger zum Einsatz kommenden Lösungen und der immer einfacheren Nutzung über bestehende Internet-Verbindungen ist es unabdinglich, einen definierten Freigabeprozess zu entwickeln, alle Entscheidungen zu begründen und das Gesamtwerk zu dokumentieren. Falls personenbezogene Daten involviert sind, ergibt sich dieser Zwang schon aus der EU-DSGVO. Sind Kundendaten von der externen Verarbeitung betroffen, dann gelten die Verträge mit den Kunden, und zuletzt der vielleicht entscheidende Punkt: Das Unternehmen selbst hat ein ureigenes Interesse daran, zu wissen, wo das Firmen-Know-how liegt, wie es geschützt wird und wie es im Zweifelsfall auch wieder zurückgeholt werden kann.

Der erste Ansprechpartner für jeden Fachbereich, oder auch für die Experten aus der IT-Abteilung, ist diejenige Person, die den besten Überblick über die bereits eingesetzten Applikationen, Services und Prozesse im Unternehmen



hat. In manchen Firmen nennt sich diese Rolle »Globaler IT-Architekt« oder »IT-Architekt« – manchmal übernimmt diese Aufgabe auch der »Manager Digitalisierung«. Die Dringlichkeit, diesen Schritt zu gehen, ergibt sich schon alleine daraus, weil die Nutzung von öffentlichen Cloud-Lösungen sehr einfach ist. So kann der Einkauf in der Zweigniederlassung Berlin mit kleinem Geld ein Cloud-Start-up in Göteborg für die Verarbeitung von Daten beauftragen, während parallel die Niederlassung in München für die gleiche Aufgabe einen Cloud-Betreiber in Indien beauftragt. Wenn es niemanden gibt, der darüber die Hoheit hat, dann ist Unsicherheit und auch unnötig hohen Kosten Tür und Tor geöffnet.

Hat der Globale IT-Architekt die Cloud-Lösung abgenickt, dann kommt bereits der Datenschutz ins Spiel. Die Prüfung, ob personenbezogene Daten involviert sind, ist damit eine Aufgabe, die zu den ersten überhaupt gehört. Hat der Datenschutzbeauftragte alle Informationen vorliegen, dann berät er **vorab** nicht nur dahin gehend, ob eine solche Lösung überhaupt gesetzeskonform ist, sondern auch über die Technisch-Organisatorischen Maßnahmen, die zu treffen sind. Diese wiederum hängen stark von der Art und damit der Kritikalität der betroffenen, personenbezogenen Daten ab.

Hat der Datenschutzbeauftragte zugestimmt oder sind keine personenbezogenen Daten betroffen, dann stellt sich als Nächstes die Frage, welchen Wert die Daten für das Unternehmen haben. Ist per Richtlinie festgelegt, dass streng vertrauliche Daten nicht für den Einsatz in öffentlichen Clouds geeignet sind, dann scheiden diese bereits automatisch aus. Das Gleiche kann für bestimmte Datenarten gelten auch unabhängig von deren Einklassifizierung. Dazu können z.B. Kundendaten gehören oder auch Daten, die ein bestimmtes Produkt betreffen, von dem sich das Unternehmen viel für die Zukunft erhofft. Der Ansprechpartner, sowohl für die Datenschützer als auch bei der Klassifizierung der Daten, ist immer der Risikoeigentümer, also diejenige Person, die in letzter Instanz über den Umgang mit den Daten bestimmen kann.

Wenn alle Hürden genommen wurden, dann spätestens ist auch die IT-Security mit im Spiel. Die Vorgaben vom Datenschutzbeauftragten und der Schutzbedarf der Daten geben vor, welche Maßnahmen zur Übertragung der Daten und welche Maßnahmen zur Überprüfung des Cloud-Providers zu treffen sind. Während die Übertragung relativ leicht sicher gestaltet werden kann, ist die Sicherstellung von Vertraulichkeit, Verfügbarkeit und Integrität



beim Anbieter schwerer zu kontrollieren. Mögliche Maßnahmen beschränken sich deshalb auch auf vorgezeigte Zertifikate, Penetrationstests oder Vor-Ort-Audits.

9.6 Betrieb von Firewalls

In der digitalen Welt ist eine Firewall ein Computer, der das interne Netzwerk einer Firma vor den böswilligen Hackern, räuberischen Kriminellen und sonstigen Übeltätern schützt, die überall im Internet herumlungern.

Bruce Schneier in »Secrets & Lies«

Eine Firewall separiert Netzwerke mit dem Ziel, den Verkehr zwischen diesen Netzwerken zu reglementieren. Firewalls gibt es heute in verschiedenen Ausprägungen, die jeweils einem avisierten Zweck dienen. Die häufigsten Anwendungsfelder sind dabei:

- Die Unternehmens-Firewall trennt das interne Unternehmensnetzwerk von externen Netzwerken wie dem Internet.
- Eine Proxyserver-Firewall reguliert den Zugang zum Internet. Häufig konzentriert sie sich auf den Zugriff von Web-Inhalten, auf die von Arbeitsplatzrechnern aus zugegriffen wird. Neben dem Ermöglichen des Zugangs spielt in diesem Fall auch die Authentifizierung und Autorisation von Benutzern eine Rolle.
- Die Personal Firewall wird auf Arbeitsplatzrechnern oder auch Servern installiert, um den Netzwerzkzugriff von außen (*inbound*) auf diese Geräte einzuschränken. In einer hohen Sicherheitsstufe werden alle Verbindungsversuche von außen automatisch abgewiesen, und nur der Arbeitsplatzrechner oder Server selbst kann Verbindungen aufbauen (*outbound*). Häufig sind Personal Firewalls Bestandteil von Antiviruspaketlösungen oder des Betriebssystems.
- Interne Firewalls segregieren besonders zu schützende Netzwerke gegen den Rest des Unternehmensnetzes. Besonders zu erwähnen sind dabei der Schutz kritischer IT-Systeme und der Schutz von Produktionsnetzen. Ein typisches Beispiel für den ersten Fall ist die Abtrennung eines SAP-Datenbankservers vom Rest des Netzwerks durch eine regelbasierte Firewall. Da es nicht unbedingt erforderlich ist, dass Endbenutzer direkt auf einen solchen Datenbankserver zugreifen, würde das Regelwerk den Zugriff auf



Systeme wie z.B. Applikationsserver etc. beschränken. Dadurch verringert sich die Angriffsfläche dieser wichtigen Systeme. Im Bereich der Produktionsnetze wiederum ist das Risiko für Schwachstellen besonders hoch, da viele produktionsnahe Computer schwer in das unternehmensweite Patchmanagement einzubinden sind. Daher ist es sehr wichtig, alle für die Produktionslinie relevanten Systeme zu identifizieren, diese in einem gemeinsamen Netz zu verwalten und das Netz gegen den Rest des Netzwerks abzusichern. Auf diese Art und Weise wird das Überspringen von Schadsoftware wie z.B. WannaCry, die auch heute noch sporadisch in Unternehmen auftaucht, zuverlässig verhindert. Ein solcher Virus, der in der Lage ist, Produktionsmaschinen zu verschlüsseln und damit unbrauchbar zu machen, zeigt am besten das Risiko und die abzuleitenden Maßnahmen auf.

- In Routern für den Heimgebrauch werden zusätzlich Firewall-Funktionen verbaut, um das Heimnetzwerk gegenüber Zugriffen aus dem Internet zu schützen.

Weitere Firewall-Produkte werden bei verschiedenen Applikationen mitgeliefert. So bieten viele VPN-Produkte die Möglichkeit, eine Software-Firewall zu installieren, um den Zugriff vom Laptop aus, der sich z.B. in einem Internet-café befinden kann, in das Unternehmensnetzwerk abzusichern.

Wichtig

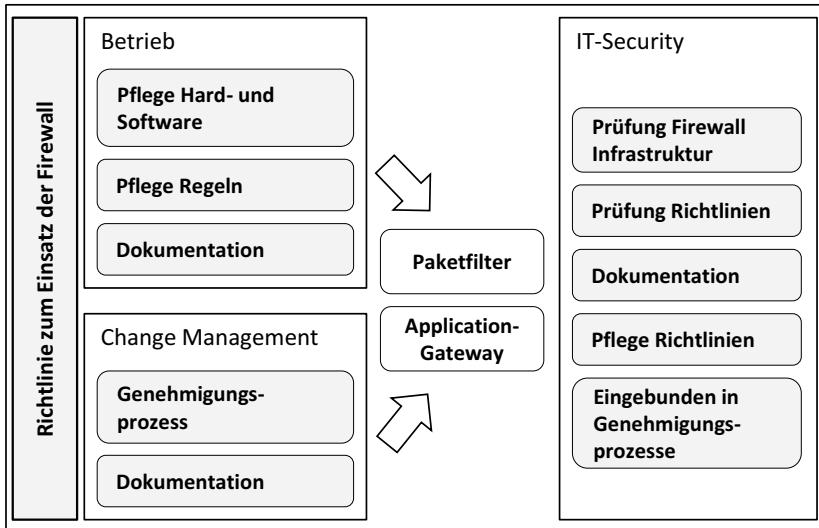
Die Definition vom Unternehmensnetzwerk als dem sicheren Netzwerk und dem Internet als Angriffsplattform von Hackern hat sich überlebt. Ein Großteil von Angriffen erfolgt aus dem eigenen Netzwerk heraus. Damit verlagert sich die letzte Verteidigungslinie bis an die einzelnen IT-Systeme und die eigenen Prozesse heran. Dem IT-Security-Management fällt die Aufgabe zu, diese Vielzahl von Einzelsystemen und die Prozesse sowie alle Schnittstellen durch Implementierung entsprechender Prozesse und Maßnahmen abzusichern.

Der Ansatz, Firewalls nur als Abgrenzung zu fremden, also nicht vom eigenen Unternehmen kontrollierten Netzen zu betrachten, ist nicht mehr aktuell. Die Separierung eigener Netze gewinnt an Bedeutung. Dabei kann es sich um ein internes Netzwerk handeln, in dem Server angesiedelt sind und auf



KAPITEL 9 – TECHNISCHE IT-SECURITY

die nur sehr eingeschränkt zugegriffen werden soll, oder aber auch ganze Unternehmenssteile, die sich im Gesamtverbund sicherheitstechnisch abschotten müssen.



9

Abbildung 9.3: Aufgaben beim Betrieb von Firewalls

Das IT-Security-Management beeinflusst alle Aspekte des Firewall-Managements, siehe Abbildung 9.3. Das beginnt bei der Evaluierung und Auswahl eines Produkts, reicht über den Betrieb und die Überprüfung bis hin zu Themen der Ausfallsicherheit in Form von Notfallprozeduren. Als zentrales Sicherheitsprodukt hat eine Firewall einen großen Einfluss auf das allgemeine Sicherheitsniveau eines Unternehmens. Hat ein Unternehmen z.B. mehrere Verbindungen zum Internet oder Zugänge mittels Wireless-Komponenten, so entscheidet das schwächste Glied über das allgemeine Sicherheitsniveau. Aus diesem Grund müssen alle sich im Einsatz befindlichen Firewalls unter gemeinsamen Gesichtspunkten betrachtet werden.

9.6.1 Paketfilter und Application-Gateways

Es existiert keine allgemein anerkannte Definition, in welche Kategorien Firewalls zu unterteilen sind. Hinter vielen Firewall-Gattungen verstecken sich letzten Ende Markenbezeichnungen der großen Hersteller. Eine grobe Einteilung hat NIST vorgenommen, und da sie sehr generisch ist, soll sie als



Richtschnur für die weiteren Ausführungen dienen. Nachzulesen sind diese Definitionen im NIST-Dokument 800-10. Diesem folgend existieren, neben Personal Firewalls auf den Arbeitsplatzrechnern, mindestens drei weitere Kategorien. Zum einen die **Paketfilter-Router**, die einfache Regelwerke zum Steuern des Netzwerkverkehrs nutzen und schon sehr lange genutzt werden. Diese Router haben den Vorteil, dass sie gerade wegen ihrer Einfachheit sehr schnelle Durchsätze bieten. Der Nachteil dieser Router liegt darin, dass nur die Verbindungen aufgebaut werden, die von vornherein explizit per Regel freigegeben wurden. Wenn man sich den Zugriff per Webbrowser im Internet vorstellt, dann wird es schon schwierig, wenn man nicht alle möglichen Kommunikationsbeziehungen per Regel abbilden möchte. Dieses Dilemma lösen die **Stateful-Inspection**-Firewalls. Diese Firewalls speichern die Daten des Zugriffs auf eine Webseite, und wenn diese im Gegenzug antwortet, werden diese Pakete zugelassen, auch wenn keine diesbezügliche Regel für diesen Inbound-Verkehr existiert. Die dritte vom NIST aufgeführte Kategorie ist die der **Proxyserver**. Ein Proxyserver ist eine sichere Art, den Übergang zwischen Netzwerken zu reglementieren. Er stellt sich quasi als Mittelsmann zwischen die Netzwerke und leitet, im Gegensatz zu den anderen Arten an Firewalls, nicht durch, sondern nimmt selbst Kontakt zur Gegenseite auf. Das funktioniert aber nicht für alle Arten von Netzwerkverkehr und die ersten Proxyserver funktionierten deshalb auch nur für Protokolle wie Telnet oder FTP. Heute existieren Proxyserver für eine Vielzahl von Applikationszugriffen. Aufgrund des Overheads bei solchen Systemen ist der Durchsatz bei diesen Firewalls im Allgemeinen niedriger als bei den anderen Kategorien.

Hinweis

Die eben beschriebenen Typen an Firewalls werden häufig in einer Software auf einer Hardware parallel betrieben. So werden Proxy-Funktionalitäten und Applikations-Firewall-Dienste auf Stateful-Inspection-Firewalls implementiert, um den Zugriff auf Daten im Internet zu kontrollieren.

Da Firewalls aktive Netzwerkkomponenten sind, kann man diese auch immer aus der Perspektive des TCP/IP-OSI-Modells betrachten. Ganz oben, auf Schicht 7, finden sich die Applikations-Firewalls, die üblicherweise aus der Kategorie Stateful Inspection oder Proxyserver stammen.



KAPITEL 9 – TECHNISCHE IT-SECURITY

Rang	Name	Aktion	Protokoll	Quelle	Ziel
1	Zugang Firma ABC	Erlauben	UDP/1092	192.168.0.12	11.192.83.12
2	UNI Stuttgart	Erlauben	TCP/21	192.168.2.37	129.69.221.130
3	VPN Fa. XYZ	Erlauben	UDP/500	192.168.0.12	121.130.22.190
4	VPN Fa. XYZ	Erlauben	UDP/4500	192.168.2.37	121.130.22.190

Abbildung 9.4: Beispielhafte Zugriffsliste einer Firewall

Dem Modell folgend haben Paketfilter-Firewalls, die auf den unteren Ebenen arbeiten, die Einschränkung, dass ausschließlich die Protokolle TCP, IP, UDP und ICMP betrachtet werden. Anwendungsprotokolle der siebten Ebene des TCP/IP-OSI-Modells können nicht untersucht werden. Damit arbeitet ein Paketfilter nicht anders als ein Router mit der eingebauten Funktionalität, Datenpakete auf ihre Zieladresse und ihren Zielport zu untersuchen und gegebenenfalls zu verwerten (*packet drop*).

9

Ein wichtiges Protokoll auf der siebten Ebene ist HTTP. Um den Datenverkehr so weit analysieren zu können, um festzustellen, ob auf dem klassischen Port 80 von HTTP auch wirklich HTTP übertragen wird, ist eine Application-Firewall erforderlich. Diese muss für jedes Protokoll, das auf der Anwendungsschicht kommuniziert, einen Proxy installiert haben. Dieser untersucht nicht nur den Header der Datenpakete, sondern auch deren Inhalt und versteht dessen Funktion. Bei HTTP ist genau festgelegt, wie ein Browser mit einem Webserver kommuniziert. Aus diesem Grund muss der Proxy (dabei handelt es sich um ein Stück Software auf der Firewall) einige der ausgetauschten Pakete filtern und auswerten. Daraufhin kann er ermitteln, ob hier wirklich HTTP-Datenverkehr stattfindet und, falls nicht, diesen verwerten.

Hinweis

In die gleiche Kategorie zählt man auch die Next-Generation-Firewalls (NG). Auch sie untersuchen nicht nur die Kommunikationsbeziehungen zwischen Quelle und Ziel, sondern nehmen auch den Inhalt der übertragenen Pakete in Augenschein und untersuchen ihn auf verdächtige Muster. Diese Funktionsweise ist eng mit der eines Intrusion-Detection-Systems (IDS) verwandt.

Damit erweitern sich die Möglichkeiten der Datensicherheit immens. Es steht nicht mehr die Frage im Vordergrund, ob Quelle x mit Zielsystem y sprechen



darf, sondern ob die beiden Kommunikationspartner dabei auch das erwartete Protokoll verwenden. Es ist ein Leichtes, aufseiten des Arbeitsplatzrechners weitgehend beliebigen Datenverkehr über den Port 80 (HTTP) umzuleiten (*redirect*). Sofern der Host auf der Gegenseite dies erwartet, könnte z.B. ein FTP-Datentransfer über diesen Port geleitet werden, und die Paketfilter-Firewall fände daran nichts Anstößiges.

Neben HTTP- und FTP-Proxies gibt es weitere, die zum Teil für ganz bestimmte Applikationen zugeschnitten sind. Kennt man den generellen Ablauf der Kommunikation, dann ist es auch möglich, einen dafür passenden Proxy zu entwickeln.

Mithilfe eines Application-Gateways ist eine weitere interessante Möglichkeit nutzbar, und zwar die, Benutzer für Applikationen im Internet zu berechtigen. Während ein Paketfilter als Quelle eine IP-Adresse sieht, kann eine Proxysoftware so entwickelt werden, dass eine Anmeldung durch eine Person erforderlich ist. Nutzt man auf diese Weise eine Application-Firewall innerhalb des internen Netzwerks, um z.B. die Administrationsumgebung der Produktionssysteme abzuschotten, so könnte ein Proxy die Zulassung des Datenverkehrs davon abhängig machen, dass sich nur Benutzer, die sich in einer definierten Gruppe befinden, über den Proxy an den Administrationsservern anmelden können. Die Steuerung der Gruppe könnte dann ein Benutzerverzeichnis wie die Active Directory Services von Microsoft übernehmen.

Grundsätzlich kann man sagen, dass der Einsatz einer Application-Firewall einen größeren Schutz und eine höhere Flexibilität bietet als ein reiner Paketfilter und dass die Kontrolle auf Ebene der Benutzer ebenso höher zu bewerten ist als die Kontrolle auf Ebene von IP-Adressen. Welche Firewall man einsetzt, wird damit wieder von der Klassifizierung der Daten abhängen, die über Netzwerkgrenzen hinweg übertragen werden sollen, und somit direkt von einer entsprechenden Risikobewertung.

9.6.2 Firewall-Regelwerk

Das Regelwerk einer Firewall (unabhängig davon, ob es sich um einen Paketfilter oder um eine Application-Firewall handelt) ist das Kernstück des Berechtigungsmanagements. Damit setzt auch eine Überprüfung, ein Audit, primär auf dem Regelwerk auf. Das gestaltet sich aber nicht ganz so einfach. Eine Firewall, deren Regelwerk über Jahre gewachsen ist, kann viele Hundert bis einige Tausend Einträge beinhalten. Wenn man dazu bedenkt, dass haupt-



sächlich auf Basis von IP-Adressen und Ports gearbeitet wird, bekommt man schnell ein Gefühl für die Komplexität der Aufgabe.

Es ist wichtig, bei der Einrichtung und Administration von vornherein ein paar wichtige Grundregeln zu beherzigen:

- Eine stringente Namenskonvention ist erforderlich, um Hosts schnell und einwandfrei identifizieren zu können. Das macht aber nur dann Sinn, wenn nicht mit IP-Adressen, sondern mit Hostnamen gearbeitet wird.
- Hosts werden grundsätzlich in Gruppen zusammengefasst. So gehören alle internen Mailserver, die mit einem externen Mail-Gateway auf die gleiche Art und Weise kommunizieren müssen, in eine Gruppe, die dann auf dem Regelsatz berechtigt wird, anstelle jedes einzelnen Mailservers.
- Diejenigen Regeln, die zeitkritischen Datenverkehr regulieren, gehören an den Anfang des Regelwerks. Da im Normalfall jedes Regelwerk sequenziell so lange abgearbeitet wird, bis eine passende Regel gefunden ist, die die Verbindung entweder zulässt (*allow*) oder verbietet (*deny*), dauert dies umso länger, je weiter unten im Regelwerk sich diese Regel befindet.
- Um die Durchsatzgeschwindigkeit der Firewall zu erhöhen, kann man als anderen Weg auch möglichst wenige Regeln erstellen. Der Nebeneffekt ist dabei der, dass die Übersicht besser gewahrt und die Überprüfung des Regelwerks deutlich vereinfacht wird.
- Die letzte Regel heißt »*drop*« oder »*deny all*«. Eine Datenverbindung, die über das gesamte Regelwerk geprüft wurde, ohne eine Entsprechung zu finden, wird schlussendlich abgebrochen. Damit werden alle Verbindungen, bei denen niemand daran gedacht hat, sie mit einer Regel zu belegen, aus Sicherheitsgründen schlussendlich fallen gelassen (*drop*).
- Eine Firewall kann die erfolgreichen und abgelehnten Zugriffe protokollieren. Das kann schnell zu einer riesigen Datenmenge anwachsen, und deshalb ist es erforderlich, sich im Vorfeld darüber Gedanken zu machen, welche Ereignisse von welchen Quell- und Zielsystemen protokolliert werden sollen. Für die Belange der IT-Security stehen fehlgeschlagene oder erfolgreiche Verbindungsversuche von außen (*inbound*) ganz oben auf dieser Liste.
- Ein regelmäßiges Audit überprüft das Regelwerk auf Stimmigkeit, doppelte Einträge und veraltete Namen. Wie bei anderen Audits auch ist es wenig sinnvoll, dieses Audit von den Betreuern der Firewall durchführen zu lassen.



sen. Eine externe Firma damit zu beauftragen und im Zuge der erforderlichen Diskussionen eine aktuelle Dokumentation zu erstellen, ist der sicherere Weg.

- Neben dem Regelwerk müssen auch die aufgelaufenen Verbindungsprotokolle überprüft werden. Dabei werden die erfolgreichen und fehlgeschlagenen Verbindungen analysiert. Da dies bei größerem Datenaufkommen kaum vollständig möglich ist, empfiehlt es sich, das Augenmerk vor allem auf kritische Verbindungen zu werfen.

Neben den aufgeführten, grundsätzlichen Verhaltensregeln ist es vor allem in großen Unternehmen entscheidend, von vornherein einen strikten Firewall-Standard festzulegen und konsequent einzuhalten. Die Überprüfung eines Dutzends Firewalls, die alle unterschiedlich konfiguriert sind und vielleicht sogar von verschiedenen Herstellern stammen, ist um ein Vielfaches teurer, als wenn genau ein Hersteller und eine Konfiguration zum Einsatz kommen. Werden auch alle Updates und Upgrades zeitnah parallel durchgeführt, dann genügt es unter Umständen, eine exemplarische Firewall in jährlichen Abständen zu auditieren.

9.6.3 Internet-Proxyserver

Sollen Mitarbeiter nicht direkt über die Firewall auf Dienste im Internet zugreifen, so platziert man sinnvollerweise einen Internet-Proxyserver zwischen Arbeitsplatz-PC und Firewall. Der Proxyserver hat dabei die Aufgabe, den Benutzer zu authentifizieren und gegebenenfalls für den Zugriff zu autorisieren. Als zentrale Instanz ist es damit auch möglich, Zugriffsdaten zu protokollieren und Sicherheitssoftware wie z.B. Virenscanner zu implementieren.

Damit handelt es sich bei einem Internet-Proxyserver um eine auf den Internetzugang spezialisierte Proxyserver-Firewall. Es kann sich dabei um dedizierte Systeme handeln oder aber um einen Internet-Proxy, der quasi als Modul auf einer Application-Firewall implementiert wird.

Folgende Möglichkeiten bieten Internet-Proxyserver – in diesem Fall wird von dedizierten Systemen ausgegangen – beim Einsatz im Unternehmen:

- Sie stehen physisch zwischen der Firewall und dem Arbeitsplatz-PC und bilden, insbesondere wenn sie mit zusätzlicher Sicherheitssoftware wie Virenscannern ausgerüstet sind, eine weitere Sicherheitsschicht. Nach



außen hin stellt sich der Proxyserver als Kommunikationspartner dar und kann Zugriffe abblocken, die vom Internet aus über die Firewall initiiert werden.

- Einige Produkte sind in der Lage, neben den weitverbreiteten Protokollen HTTP, HTTPS und FTP auch andere Protokolle zu filtern. Damit wird es möglich, auch den Zugriff von Applikationen auf Dienste im Internet über einen zentralen Proxy zu lenken und somit den Zugriff über Anmeldeparameter wie Benutzer und Passwort zu steuern.
- Über den Proxyserver kann die Autorisierung derjenigen Mitarbeiter abgewickelt werden, die Zugriff auf Inhalte im Internet erhalten sollen.
- Internetzugriffe können auf dem zentralen Proxyserver protokolliert werden. Dabei sind die datenschutzrechtlichen Rahmenbedingungen zu beachten, ebenso die Vorgaben aus den Betriebsvereinbarungen mit dem Betriebsrat.
- Zugriffe und heruntergeladene Dateien können in einem Cache vorgehalten werden, um erneute Zugriffe schneller zur Verfügung stellen zu können und die Auslastung des Netzwerks zu reduzieren.

9

9.7 Internetzugang und Nutzung von E-Mail

Die Nutzung von E-Mail sollte genauso über Richtlinien geregelt werden wie der Zugang von Mitarbeitern zum Internet. Das berührt in beiden Fällen sowohl direkt die Aufgabe der IT-Security, den Schutz von sensiblen Informationen sicherzustellen, wie auch arbeits- und datenschutzrechtliche Fragestellungen. So ist bei E-Mail zu beachten, dass im Falle, dass die private Nutzung von Internet und E-Mail zugelassen ist, eine Reihe von gesetzlichen Regelungen greifen, die bei dem generellen Verbot der privaten Nutzung nicht anzuwenden sind. Das röhrt maßgeblich von der möglichen Vermischung privater und geschäftlicher Daten her.

Zu den wichtigsten zu beachtenden Gesetzen gehören neben der EU-DSGVO das Telekommunikationsgesetz und das Telemediengesetz. Sollen Zugriffsdaten und Inhalte von E-Mails ausgewertet werden können und soll dies über den Zugriff auf anonymisierte oder zumindest pseudonymisierte Daten zur technischen Störungsbehebung hinausgehen, so ist die Vorschrift, dass ausschließlich eine dienstliche Nutzung dieser Medien gestattet ist, eine wichtige



Voraussetzung. Ein Freifahrtschein ist sie trotzdem nicht. In jedem Fall muss abgewogen werden, ob das Interesse des Arbeitgebers am Schutz vor missbräuchlicher Nutzung das Recht auf Wahrung der Persönlichkeitsrechte des Arbeitnehmers überwiegt. Das Stichwort hier ist das »Verhältnismäßigkeitsprinzip«. Letztendlich wird dies eine Entscheidung sein, die fallweise getroffen werden muss.

Beiden Themen, dem Internetzugriff und der Nutzung von E-Mail, ist gemeinsam, dass alle Regelungen mit dem Betriebsrat abgestimmt sein sollten und vorzugsweise durch entsprechende Betriebsvereinbarungen geregelt gehören. So ist die Verwendung von Protokolldaten aus dem Internetverkehr eine heikle Angelegenheit, die dadurch abgefertigt werden kann, dass die genauen Methoden zur Auswertung und die Vorgehensweise in einer Betriebsvereinbarung definiert sind.

9.7.1 Risikofaktor E-Mail

Der Empfang und das Versenden von E-Mail ist integraler Bestandteil vieler Unternehmensprozesse. Abhängig vom Geschäftszweck kann dieser Vorgang von der Wichtigkeit her bis in die Einstufung »unternehmenskritisch« reichen. So kann ein Unternehmen, das sich mit der Annahme von Bestellungen und dem Versand von Gütern beschäftigt, nur wenige Tage oder gar nur Stunden überleben, wenn das Kommunikationsmittel E-Mail ausfällt. Neben dem Risiko des Ausfalls der Funktionalität E-Mail bringt das Medium an sich weitere Risiken für die Datensicherheit mit sich. So können zunächst vier Sichten definiert werden, die verschiedene Bedrohungen beschreiben:

- Der Inhalt von Standard-E-Mails ist aufgrund des verwendeten Internetprotokolls SMTP nicht verschlüsselt. Solange also Inhalte nicht per verschlüsseltem Attachment angehängt werden oder aber die Verschlüsselung der kompletten E-Mail vorgenommen wird, können E-Mails abgefangen und der Inhalt ausgelesen werden. Zudem ist es leicht möglich, den Inhalt von E-Mails zu verändern oder aber deren Empfänger zu fälschen (*mail spoofing*). Der Versand kritischer Informationen mittels E-Mail muss also genau geregelt werden. So kann z.B. festgelegt werden, dass sensible Daten ausschließlich über verschlüsselte E-Mails versendet werden dürfen.
- Der Empfang oder der Versand von Schadsoftware per E-Mail ist ein weites Problemfeld. Startet der Benutzer oder aber das Mail-Programm selbst



eine Schadsoftware, die mit einer E-Mail mitgeschickt wird, so sind der Arbeitsplatzrechner und alle verbundenen Datenquellen und erreichbaren Gerätschaften im Netzwerk gefährdet. Dieser Problematik kann mit entsprechenden Handlungsanweisungen wie »Niemals eine Applikation öffnen, die als Anhang verschickt wird« und Antivirenprogrammen auf dem Mailserver und/oder dem Arbeitsplatzrechner begegnet werden. Die Auswirkungen einer solchen Infektion können sofort auftreten, z.B. durch das Löschen von Daten, oder aber unbemerkt im Hintergrund tätig werden, wie bei Trojanern, die Passwörter abfangen.

- E-Mails bestimmter Größe oder wenn diese in sehr hoher Zahl empfangen werden, können das E-Mail-System an sich zum Erliegen bringen. Diesen Angriff nennt man »Denial of Service«- oder DOS-Angriff.
- E-Mails, deren Empfang nicht gewünscht ist, also sogenannte »Spam-Mails«, haben einen negativen Einfluss auf die Produktivität der Mitarbeiter und unter Umständen auch auf die Mail-Infrastruktur, deren Funktionieren ähnlich wie bei DOS-Angriffen durch Überlastung gestört werden kann.

9

9.7.2 Verschlüsselung von E-Mails

Für die Verschlüsselung von E-Mails empfiehlt es sich, Hardware und/oder Software einzusetzen, die von Endgerät zu Endgerät oder Unternehmensnetzwerk zu Unternehmensnetzwerk jede E-Mail automatisch verschlüsselt. Dafür sind entsprechende S/MIME- und PGP-Lösungen auf dem Markt. Im Falle der Verschlüsselung von Unternehmensnetzwerk zu Unternehmensnetzwerk können nach Austausch eines Unternehmensschlüssels alle E-Mails, die zwischen den konfigurierten Unternehmen versendet werden, automatisch verschlüsselt werden.

Ein weiteres Verfahren, das sich auf breiter Front durchgesetzt hat, ist die Verschlüsselung per Transport Layer Security (TLS). Dabei handelt es um eine einfach zu implementierende Art des Schutzes, der den Transport zwischen den E-Mail-Servern adressiert.

Trotz der technischen Möglichkeiten, die verfügbar sind, wird die Verschlüsselung von E-Mails auch heute noch viel zu selten genutzt. Viele Unternehmen verschicken nach wie vor ihre Daten unverschlüsselt, und im privaten Umfeld ist dies immer noch der Standard. Das liegt zum Teil daran, dass es mehrere mögliche technische Vorgehensweisen gibt, die zueinander inkom-



patibel sind. Zudem scheuen Unternehmen den Aufwand, eine Infrastruktur aufzubauen und die zur Verschlüsselung erforderlichen Schlüssel zu verwalten. In einem mittelständischen Betrieb kann die Anzahl an Mail-Partnern schnell die Grenze von 100 Unternehmen überschreiten. Vor der Einführung einer Verschlüsselungstechnik sollte also zunächst festgestellt werden, mit welchen Partnern sensible Daten ausgetauscht werden, um dann herauszufinden, welche Lösung tragfähig und zukunftsfähig ist.

9.7.3 Risikofaktor Internetbrowser

Der Internet-Browser ist die Software im Unternehmen, die jeden Benutzer mit Zugang zum Internet direkt mit den Inhalten im Internet verbindet. Aus diesem Grund ist die Browsersoftware Angriffen aus dem Internet zunächst einmal direkt ausgesetzt. Selbst wenn der Benutzer hinter einer Firewall angesiedelt ist, wird diese nicht verhindern, dass Inhalte heruntergeladen und anschließend vom Browser interpretiert werden. Dazu gehören Textinformationen genauso wie kleine Videos, Java-Anwendungen oder Flash-Animationen. Jede dieser Anwendungen bzw. Darstellungsformen erfordert speziell zugeschnittene Software, die zu jedem Zeitpunkt auf einem sicheren Stand sein muss. Also muss neben dem Browser selbst auch jede weitere in seinem Kontext ablaufende Software stetig auf dem neuesten Stand gehalten werden.

Neben dem Aufwand für das Update selbst kann dies zu Problemen hinsichtlich der Kompatibilität führen. Funktioniert eine Software, die in einem Browserfenster abläuft, mit einer älteren Version von Java klaglos, so kann diese eventuell ihren Dienst einstellen, falls die neueste Version installiert wird. In diesem Fall muss eine Risikoabwägung stattfinden mit der Entscheidung, eventuell nicht zu aktualisieren, um die Lauffähigkeit nicht negativ zu beeinflussen.

Mit den komplexer werdenden Anwendungen, die ein Browser verarbeiten kann, und der steigenden Leistungsfähigkeit von Rechnern steigen auch die Möglichkeiten, umfangreiche Schadprogramme über einen Standardbrowser ausführen zu lassen. Codes, die in infizierte Webseiten eingebettet werden, oder infizierte Browsererweiterungen dienen dazu, diese Programme zu starten. Dabei kann es sich z.B. um Java-Applikationen handeln, die auf dem Rechner des Benutzers unbemerkt Crypto-Währungen »minen« oder Informationen ausspähen.



9.8 Penetrationstests

In einem Unternehmen, in dem die IT-Security-Organisation ihre Hausaufgaben gemacht hat, existieren Regelungen für die meisten technischen Systeme und die darauf installierte Software. Außerdem hat eine weitreichende Standardisierung der IT-Systeme stattgefunden. Trotz all dieser Maßnahmen und gelebten Prozesse wird es sich dennoch immer nur um eine Annäherung an eine umfassende Informationssicherheit handeln.

Ein weiterer wesentlicher Schritt, das Sicherheitsniveau zu verbessern, ist der Schritt von der mehr theoretischen Erfassung von Bedrohungen und der Definition von Maßnahmen hin zu einer technischen Untersuchung der IT-Systeme mittels Penetrationstests. Es ist vergleichbar mit dem Schritt vom Zeichenbrett zum ersten Prototyp: Man weiß im Vorfeld nicht so genau, was einen wirklich erwartet und was schlussendlich dabei herauskommt. Penetrationstests sind eine begleitende Maßnahme. So kann die technische Suche nach Schwachstellen das IT-Risikomanagement entscheidend unterstützen und mit Anhaltspunkten versorgen.

Hinweis

Genauso wie alle anderen Prozesse der IT-Security sind auch Penetrationstests keine einmalig durchgeführte Maßnahme, sondern folgen ebenso dem Plan-Do-Check-Act-Zyklus. In der Wiederholung von Tests und der laufenden Verbesserung des untersuchten Gegenstands liegt das Verbesserungspotenzial für das allgemeine Sicherheitsniveau.

Ein Penetrationstest beschäftigt sich mit der Frage, inwieweit ein Angreifer die Schwachstellen eines IT-Systems erkennen und ausnutzen kann, um an Daten zu gelangen, für deren Zugriff er nicht autorisiert ist. Eine weitere Spielart ist die Frage, inwieweit ein Angreifer die Verfügbarkeit negativ beeinflussen und durch den Ausfall Kosten verursachen kann.

Penetrationstests verlangen ein hohes Maß an Detailwissen, was die technischen Zusammenhänge in Bezug auf die Zielsysteme angeht. Dieses Wissen ist, und das spiegelt sich auch an der Arbeitsplatzbeschreibung eines typischen Managers IT-Security wider, nicht in jedem Fall die Kernkompetenz des Managers IT-Security. Natürlich sollte er ein grundlegendes Verständnis für



Betriebssysteme, Anwendungsprogramme und Netzwerke mitbringen. Aber zu wissen, wie man TCP/IP-Datenpakete so manipulieren kann, um damit Denial-of-Service-Angriffe ausführen zu können, wird meistens Experten überlassen. Das liegt nicht allein daran, dass nur diese über das erforderliche handwerkliche Geschick des Durchführens von simulierten Angriffen verfügen, solche Tests sind zudem sehr komplex, und bei nicht ausreichendem Fachwissen ist es leicht, Schwachstellen zu übersehen oder ungewollt Schaden anzurichten. Trotzdem, und das ist wichtig zu verstehen, ist es durchaus üblich, dass vier beauftragte Firmen auch vier verschiedene Wege finden, ein Zielsystem zu kompromittieren.

Trotz der eben genannten Einschränkungen gibt es keinen besseren Weg, die technischen Aspekte der IT-Security kennenzulernen, als sich mit der Thematik Penetrationstests bis hinein in die tiefsten Schichten der Netzwerkprotokolle auseinanderzusetzen. Wenn man dies in einer Testumgebung tut, kann eigentlich nichts mehr schiefgehen.

Es empfiehlt sich, die folgenden Phasen strukturiert zu untersuchen:

- **Das Sammeln von Informationen** über das Zielsystem. Um welches Betriebssystem es sich handelt, welche Version installiert ist, welche Patches aufgespielt wurden, welche Benutzer darauf berechtigt sind und welche Software bzw. Dienste darauf installiert sind, gehört zu den ersten Fragen, die man sich stellen sollte.
- **Die Untersuchung des Netzwerks** ist ein guter zweiter Schritt. Was befindet sich noch im Netzwerk des Zielsystems, wie wird es geschützt, hat das Zielsystem noch weitere Netzanschlüsse, über welche aktiven und passiven Netzwerkkomponenten erfolgt der Zugriff? Das Umfeld des Zielsystems ist häufig wichtiger als das Zielsystem selbst. Gelingt der Zugriff auf ein System im gleichen Netzwerk, dann kann unter Umständen eine interne Firewall umgangen werden, bevor der Angriff auf das eigentliche System beginnt.
- **Erkennen von aktiven Diensten.** Durch Port-Scans kann nun festgestellt werden, welche Dienste und Applikationen auf dem Zielsystem arbeiten und auf Anfragen warten. Über die geöffneten Ports wird im Weiteren die Kommunikation stattfinden und, falls möglich, auch ein Angriff. Ist es möglich, die installierte Version herauszufinden, so kann das Internet dabei helfen, eventuelle Angriffsszenarien zu entwickeln, die in der Folge ausgeführt werden können.



Für IT-Systeme, deren Überwachung durch externe Anbieter zu teuer oder im Rahmen der Risikoabwägung nicht erforderlich ist, kann die Penetration durch automatisierte Scanprogramme einen effektiven Kompromiss darstellen. Entsprechende Programme, die nicht nur einen Portscan durchführen, sondern in einem zweiten Schritt bereits versuchen, die Version der installierten und gefundenen Dienste herauszufinden, können sehr gut weiterhelfen, wenn man neue Schwachstellen, z.B. nach dem Aufspielen neuer Software oder nach Updates, finden will.

9.9 Digitale Signatur

9

Anders als bei Dokumenten, die eigenhändig unterschrieben sind, haben digitale Dokumente nicht den Status einer Urkunde. Dies wird bereits in §§ 415 ff. Zivilprozeßordnung (ZPO) und der entsprechenden Rechtsprechung festgelegt. Danach sind elektronische Dokumente aufgrund der fehlenden Schriftform und der fehlenden handschriftlichen Unterschrift keine Urkunden. Die digitale Signatur soll diesem Manko abhelfen, indem der Inhalt von Dokumenten und die Unterschrift sozusagen beglaubigt werden.

Laut § 2 (1) Signaturgesetz handelt es sich bei einer elektronischen Signatur um Daten, die anderen elektronischen Daten beigelegt oder mit diesen logisch verknüpft werden und die der Authentifizierung dienen. Die elektronische Signatur bestätigt damit also sowohl den Inhalt des digitalen Dokuments als auch den Urheber. Des Weiteren wird der Begriff des »Signatoren« weiter ausgeführt und definiert als Person oder eine sonstige rechtsfähige Einrichtung, der Signaturerstellungsdaten und Signaturprüfdaten zugeordnet sind und die im eigenen oder fremden Namen eine elektronische Signatur erstellt.

Hinweis

Der Begriff »digitale Signatur« sollte nicht synonym für den Begriff »elektronische Signatur« verwendet werden. Die Bezeichnung »elektronische Signatur« ist ein Rechtsbegriff, wie er im Signaturgesetz verwendet wird. Die digitale Signatur ist damit die Beschreibung, wie eine elektronische Signatur technisch umgesetzt wird.



Ein Unternehmen, das Rechnungen an Lieferanten stellt und dies in elektronischer Form tun möchte, kann mittels der digitalen Signatur selbst oder durch Dritte diese Dokumente mit einer Signatur versehen und somit in eine Form bringen, dass sie als Urkunde anerkannt werden.

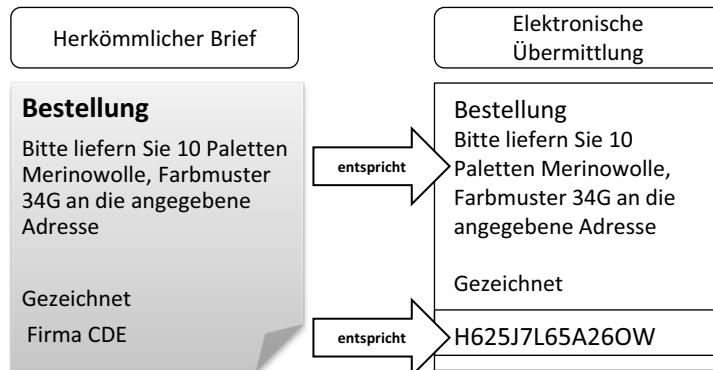


Abbildung 9.5: Gleichbehandlung von herkömmlichen Papierdokumenten und digitaler Entsprechung

9

Auch hier gibt es verschiedene Sicherheitsstufen. So existiert neben der einfachen »elektronischen Signatur« auch die »fortgeschrittene elektronische Signatur«, die entsprechend höheren Sicherheitsanforderungen genügen muss. Als dritte Ausprägung verlangt die »qualifizierte elektronische Signatur« eine fortgeschrittene elektronische Signatur, die zusätzlich auf einem qualifizierten, also überprüfbar, Zertifikat beruht.

Hinweis

Die elektronische Signatur ist abzugrenzen von der Verschlüsselung eines Dokuments. Im Falle der elektronischen Signatur wird durch Erstellung einer Prüfsumme lediglich sichergestellt, dass der Inhalt nicht verändert werden kann. Die Verschlüsselung eines Dokuments dagegen sorgt dafür, dass es nur vom Empfänger wieder entschlüsselt und in eine lesbare Form gebracht werden kann.

Der Zertifizierungsdienstanbieter, der befugt ist, Zertifikate für die qualifizierte elektronische Signatur auszustellen, muss eine ganze Reihe von Anforderungen erfüllen. Hier empfiehlt sich eine sorgfältige Prüfung, da sich ein



Unternehmen stark an einen solchen Anbieter bindet, sobald die Entscheidung getroffen wird, mit ihm zusammenzuarbeiten. Dokumente, für die sich der Einsatz einer elektronischen Signatur anbietet, haben zum Teil sehr lange Aufbewahrungsfristen, und deshalb müssen auch die Zertifikate eine entsprechend lange Laufzeit besitzen. Das und die Akkreditierung durch die Bundesnetzagentur sind weitere Qualitätsanforderungen an einen möglichen Anbieter.

9.10 Intrusion-Detection-Systeme

Ein Intrusion-Detection-System (IDS) ist eine Software, die dazu dient, Angriffe auf IT-Systeme und Netzwerke zu erkennen. Typischerweise überwacht es dazu den Netzwerkverkehr. Anders als ein Monitoring-System überwacht es nicht die Verfügbarkeit von Services und Hosts, sondern den Datenverkehr an sich und schließt aus den übermittelten Datenpaketen, ob ein Sicherheitsvorfall (*security incident*) vorliegt.

Erkannte Angriffsmuster werden in Form von Listen oder Dashboards sichtbar gemacht und stehen zur weiteren Bewertung durch den IT-Experten zur Verfügung. Damit verhält sich ein IDS passiv im Sinne von »Es überwacht aktiv, greift aber nicht aktiv ein« und letztendlich ist die Expertise des Administrators entscheidend, ob und – wenn ja – welche Maßnahmen zur Abwehr getroffen werden.

Es wird zwischen drei verschiedenen Arten von IDS unterschieden:

- **Host-basierte IDS (HIDS):** Ursprünglich entwickelt, um Vorgänge auf Großrechnern in Echtzeit überwachen zu können, überwachen sie das System, auf dem sie üblicherweise auch installiert sind. HIDS können Dateizugriffe, Zugriffe auf Speicherbereiche oder den Netzwerkverkehr überwachen. Zusätzlich können sie verwendet werden, um von Applikationen erzeugte Protokolldateien auszuwerten. In Zusammenarbeit mit dem VirensScanner sind viele dieser Systeme in der Lage, verdächtige Aktionen wie z.B. die Installation eines Root-Kits zu erkennen. Wie eine Blackbox aus einem Flugzeug dienen die Aufzeichnungen eines HIDS nach der erfolgten Kompromittierung oder nach einem erfolgreichen Denial-of-Service-Angriff zur nachträglichen Fehlererkennung und unterstützen die Analyse.



- **Netzwerkbasierte IDS (NIDS):** Die Aufgabe eines NIDS ist es, den Netzwerkverkehr zu überwachen und Muster von Angriffen zu erkennen und zu interpretieren. Die Kunst liegt darin, dass es nicht nur darum geht, bestimmte Abfolgen von Netzwerkpaketen zu erkennen, sondern auch Zusammenhänge zwischen verschiedenen Ereignissen herzustellen. So kann der Start einer Kommunikation mit einem bestimmten Netzwerkport eines Computers für sich alleine gesehen harmlos sein. Geschieht dies aber auch systematisch in gleicher Weise bei anderen Rechnern, dann kann es sich um einen großflächigen Angriff handeln. NIDS arbeiten mit Sensoren, die auf Computern oder Netzwerkkomponenten installiert werden und mit einem zentralen NIDS-System kommunizieren.
- **Hybride IDS:** Um die Abdeckung und Effektivität einer IDS-Überwachung zu steigern, werden häufig Systeme eingesetzt, die sowohl aus Komponenten bestehen, die das lokale Computersystem überwachen (HIDS), als auch aus Sensoren im Netzwerk für die Überwachung des Netzwerkverkehrs (NIDS).

Ein IDS-System kann auf zwei verschiedene Arten versuchen, Angriffe zu erkennen. Zum einen durch einen Vergleich von bekannten Angriffssignaturen mit den überwachten Netzwerksdaten und Protokolldaten, durch künstliche Intelligenz bzw. Machine Learning, und zum anderen durch eine statistische Analyse. Das Ziel der statistischen Analyse ist es, bislang unbekannte und deshalb auch nicht als Signatur verfügbare Angriffe durch mathematische Verfahren zu erkennen. Naturgemäß ist dabei die Fehlerquote höher als bei erkannten Signaturen. Auch fehlen in diesem Fall die grundlegenden Informationen, um die Art und Schwere des Angriffs feststellen zu können.

Um Angriffe zu erkennen, die nur leicht von bekannten Angriffsmustern abweichen, werden heuristische Methoden genutzt. Damit lässt sich die Wahrscheinlichkeit für eine Angriffserkennung weiter steigern.

Hinweis

Anders als ein Intrusion-Detection-System ist das Intrusion-Prevention-System (IPS) in der Lage, auf erkannte Angriffe mit im Voraus definierten Maßnahmen wie dem Abschalten von Netzwerkverbindungen zu reagieren.



Ein IDS wird zumeist in Netzwerksegmenten installiert, in denen ein Angriff wahrscheinlich oder aber risikoreicher ist. Dazu gehören Bereiche, die vom Internet aus erreichbar sind, oder aber Netzwerke, in denen sensible IT-Systeme installiert sind. Um zielgerichtet arbeiten zu können, kommen sogenannte Honeypots zum Einsatz. Ein Honeypot ist ein IT-System, das keine produktive Funktion hat, aber für einen potenziellen Angreifer verlockend aussieht. Ein IDS, das einen solchen Honeypot überwacht, kann beliebig lange Informationen über den Angreifer sammeln, ohne dass die Verfügbarkeit wichtiger Prozesse gefährdet ist.

Intrusion-Detection-Systeme haben wie alle Monitoring-Komponenten das Problem, dass eine Vielzahl an Alarmen erzeugt wird, von denen üblicherweise nur eine geringe Anzahl wirklich relevant und beachtenswert ist (*false positive*). Die Beurteilung, auf welche Meldungen reagiert werden muss und in welchem Ausmaß, kann die Software nur ansatzweise leisten. An dieser Stelle muss der Fachmann eingreifen und eine Bewertung abgeben.

9.11 Wireless LAN

Als Wireless Local Area Network (WLAN) wird ein lokales, auf Funk basierendes Netzwerk bezeichnet. Mit WLAN-Fähigkeit ist ein Ausstattungsmerkmal gemeint, das in Computern (hier vor allem Laptops), Mobiltelefonen, Tablets, Produktionsmaschinen und vielen weiteren Gerätschaften zu finden ist. Der einfache und vergleichsweise kostengünstige Aufbau eines WLAN hat dazu geführt, dass es sowohl für Privatanwender als auch für Unternehmen üblich geworden ist, ihr drahtgebundenes Netzwerk um ein WLAN zu ergänzen und damit die Reichweite und Zugriffsmöglichkeiten zu erweitern. Ist der Zugang zu einem kabelgebundenen LAN nur durch eine physische Verbindung möglich, so ist der Zugang zu einem WLAN mit entsprechenden Reatern und Verstärkern auch über viele Hundert Meter (und damit über die Sichtweite hinaus) möglich. Alle diese Möglichkeiten machen die Dringlichkeit deutlich, warum der Zugang zu einem WLAN sicher gestaltet werden muss.

Ein WLAN kann in zwei Modi betrieben werden. Zum einen kann ein einzelnes Gerät im **Ad-hoc-Modus** betrieben werden. Dieser Modus kann für den schnellen und unkomplizierten Datenaustausch benutzt werden, ist aber eher für die Techniken Bluetooth und Infrarot üblich. Dieser Modus ermög-



licht einem Angreifer den Zugriff auf das Gerät, das diese Art von WLAN aktiviert hat.

In Unternehmen wird ein WLAN vorwiegend im **Infrastrukturmodus** betrieben. In diesem Fall wird eine aktive Netzwerkkomponente implementiert, die als zentraler Ansprechpartner für Clients dient. Der sogenannte Access-Point dient dabei als Kontaktspunkt für den Client, der sich mit dem Netzwerk verbinden möchte. Um dies zu ermöglichen, sendet er laufend Datenpakete aus, die alle Informationen beinhalten, die ein Client benötigt, um sich aktiv verbinden zu können. Dazu gehören vor allem die Informationen über den Namen des Netzwerks, eine Liste mit unterstützten Übertragungsarten und die vorausgesetzte Art der Verschlüsselung.

Hat sich ein Client erfolgreich mit einem Access-Point verbunden, dann kann er direkt in das kabelgebundene Netzwerk geroutet werden. Dies wird dadurch möglich, weil auch WLAN die Sicherungsschicht (OSI-Schicht 2) verwendet.

Um die Sicherheit von WLAN-Installationen zu verbessern, sollten eine ganze Reihe von Richtlinien erlassen werden. Folgende Bereiche sollten darin enthalten sein:

- **Strahlungsleistung der Access-Points:** Je stärker die Sendeleistung, desto größer ist der Bereich, in dem potenzielle Angreifer Zugriff auf das WLAN nehmen können. Aus diesem Grund sollte die Sendeleistung nur die Stärke haben, die erforderlich ist, um die angeforderten Bereiche mit WLAN zu versorgen.
- **Bereich der Ausleuchtung:** Moderne Access-Points können nicht nur die Sendeleistung flexibel konfigurieren, sondern auch die Ausleuchtung individuell verändern. So ist es nicht immer sinnvoll, dass kreisförmig um den Access-Point Zugriff genommen wird, manchmal soll auch nur eine Halle ausgeleuchtet werden, für die eher eine keulenförmige Ausleuchtung sinnvoll wäre.
- **Vermessung des WLAN:** Die Erfassung, wo das WLAN mit welcher Stärke empfangbar ist, kann mit entsprechender Technik vorgenommen werden. Dies versetzt den Sicherheitsverantwortlichen in die Lage, Modifikationen in Strahlungsleistung und Ausleuchtung vornehmen zu können.



- **Verschlüsselungsstandard:** Die Art der Verschlüsselung bestimmt in großem Maße die Sicherheit der WLAN-Installation. So ist der WEP-Standard bereits seit einigen Jahren unsicher, und auch die WPA-Verschlüsselung mit kleinen Schlüsseln kann geknackt werden. Dazu kommt, dass die Verwendung von festen Schlüsseln (Pre-shared Keys, PSK) immer die Problematik beinhaltet, dass diese Schlüssel in fremde Hände gelangen können. Die Nutzung von Zertifikaten zur Authentifizierung von Benutzern und/oder Rechnern ist ein Standard, der heute häufig eingesetzt wird.
- **Zugang zum kabelgebundenen Netz beschränken:** Computer, die sich erfolgreich mit dem WLAN verbunden haben, können direkt in das Unternehmensnetzwerk geroutet werden. Das ist aber nicht für alle Gerätschaften erforderlich. So kann es sinnvoll sein, Barcodescanner aus dem Produktionsbereich mit einer zusätzlichen Firewall, die häufig Bestandteil eines Access-Point-Managementsystems ist, vom Netzwerk abzutrennen und nur auf einen Zielrechner zuzulassen. Das Gleiche gilt für WLAN-Installationen, die von Gästen genutzt werden.



10 IT-Risikomanagement

10.1 Kapitelzusammenfassung

Das IT-Risikomanagement bildet den Überbau über den Gesamtkomplex IT-Security-Management. Dieses Bild soll die Tatsache betonen, dass es sich bei dieser Disziplin nicht um eine abgegrenzte Einzelaufgabe handelt, sondern um eine Methodik, die in vielen Prozessen immer wieder auftaucht.

Der Einfluss und die Methoden des IT-Risikomanagements durchziehen alle Teilbereiche des IT-Security-Managements. Für das Business Continuity Management sowie für die tägliche Arbeit und die implementierten Sicherheitsprozesse stellt es zudem eine entscheidende Grundlage dar.

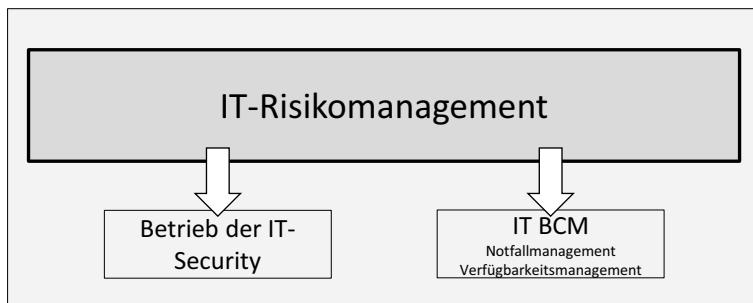


Abbildung 10.1: Primäre Abhängigkeiten von anderen Themen der IT-Security

Im Eingangskapitel wurde geschrieben, dass es die Frage nach dem »Wie« beantwortet. Also die Frage nach der Vorgehensweise eines Managers IT-Security. Das IT-Risikomanagement hilft bei der Quantifizierung von Risiken, bestimmt objektiv deren Gewichtung und entscheidet damit auch über die Art und Stärke von einzuleitenden Maßnahmen. Damit bildet es das bestimmende Element in vielen Entscheidungsprozessen.



Die Top-4-Fragen zum aktuellen Kapitel:

- Existiert eine Richtlinie zum IT-Risikomanagement? Wurde die dort beschriebene Vorgehensweise mit den Methoden des Unternehmensrisikomanagements abgestimmt?
- Liegen Aufzeichnungen und Dokumentationen vor, die die wichtigsten IT-Risiken für den Geschäftsbetrieb darstellen?
- Ist das erforderliche Handwerkszeug für ein IT-Risikomanagement vorhanden? Liegt eine Klassifizierungsrichtlinie vor und sind die Mitarbeiter damit vertraut? Wurden Bedrohungslisten erstellt und entsprechende Maßnahmenvorschläge vorbereitet? Werden zumindest die wichtigsten Unternehmenswerte anhand der Klassifizierungsrichtlinie klassifiziert?
- Werden IT-Prozesse auch über den Faktor Risikomanagement gesteuert?

10

10.2 Einführung

Das Wissen um die Risiken, denen sich ein Unternehmen und davon abgeleitet auch die IT-Abteilung, das Gebäudemanagement oder die Unternehmensplanung aussetzen, stellt die Basis für beinahe jede Entscheidung innerhalb des IT-Security-Managements dar. Nur wenn den beteiligten Parteien bewusst ist, welche Konsequenzen eine Handlung oder deren Unterlassung hat, wird es ihnen möglich sein, die richtigen Entscheidungen mit dem angemessenen Wirkungsgrad zu treffen. Das IT-Risikomanagement beschäftigt sich dabei vornehmlich mit den Risiken, die im Rahmen der Verarbeitung von Daten mithilfe von IT-Systemen auftreten können.

10.3 IT-Risikomanagement im Unternehmenskontext

In einem Unternehmen wird die oberste Stufe der langfristig angelegten unternehmerischen Planung als Unternehmensstrategie bezeichnet. Sie bildet das Bindeglied zwischen der Vision des Unternehmens und den tatsächlichen betrieblichen Erforderlichkeiten. Abgeleitet von der Vision, die eine Vorstellung des Soll-Zustands in der Zukunft beschreibt, werden somit unternehmerische Tätigkeiten abgeleitet. Die Unternehmensstrategie hat dabei einen in die Zukunft gerichteten Planungshorizont. Zum Teil besteht sie aus



Zielzuständen wie z.B. einer angestrebten Umsatzentwicklung und zum anderen Teil aus Richtlinien, die beschreiben, wie die Zielzustände konkret erreicht werden sollen. Dem unternehmerischen Risikomanagement fällt in diesem Umfeld die Aufgabe zu, Abweichungen von diesen Zielen zu vermeiden, indem Risiken kontrolliert begegnet wird.

Hinweis

Das IT-Risikomanagement ist Teil des Unternehmensrisikomanagements und gewinnt in dem Maße an Bedeutung, wie die Abhängigkeit der Kernprozesse von IT-Systemen und allgemein der Datenverarbeitung steigt.

Die IT-Strategie orientiert sich nun gleichfalls an der Unternehmensstrategie und die Richtlinien des IT-Risikomanagements wiederum an der IT-Strategie. Neben dieser strategischen Sicht des IT-Risikomanagements existiert auch eine operative Ebene, auf der ein Hauptteil des IT-Risikomanagements abläuft.

Die Strukturierung eines IT-Risikomanagements enthält somit die folgende Staffelung:

- Identifizierung von Risiken für das Unternehmen aus strategischer IT-Sicht
- Bewertung dieser Risiken auf kurz-, mittel- und langfristiger Basis
- Festlegung, wie mit den identifizierten Risiken umgegangen werden soll. Dies erfolgt zunächst auf strategischer und dann auf operativer, taktischer Ebene.

Das IT-Risikomanagement hat daraus abgeleitet die Aufgabe, Methoden zu entwickeln und umzusetzen. Dabei gilt es, auf operativer Ebene Risikomanagementprozesse zu koordinieren, ohne den Blick auf die strategischen Unternehmensziele zu verlieren.

Das IT-Security-Management wird sich in diesem Gesamtkontext maßgeblich um die Tätigkeiten kümmern, die einen Einfluss auf Schutzziele wie Vertraulichkeit, Verfügbarkeit oder Integrität haben. Da in diesem Fall IT-Systeme und die damit verarbeiteten Daten im Mittelpunkt stehen, wird der Manager IT-Security vor allem auf operativer Ebene arbeiten.

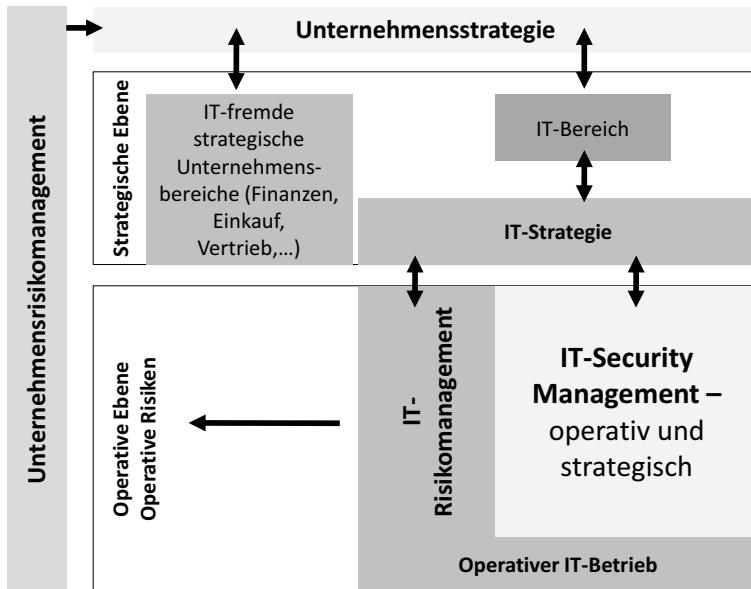


Abbildung 10.2: Einordnung des IT-Risikomanagements

10.4 Akzeptanz des IT-Risikomanagements

Damit ein IT-Risikomanagement bis zur letzten Konsequenz betrieben wird, ist es unabdingbar, dass es allgemein akzeptiert ist. In diesem Zusammenhang spricht man von Risikomanagementkultur. Neben der Richtlinie zum Risikomanagement, die den Standpunkt der Unternehmensleitung darstellt, muss ein generelles Verständnis bei allen betroffenen Parteien vorhanden sein. Insbesondere die Prozesseigentümer in den Fachbereichen müssen den Risikomanagementprozess nicht nur aktiv unterstützen, sondern häufig auch Maßnahmen umsetzen und die Konsequenzen der Risikobehandlung verantworten.

Gelebtes, also nachhaltig betriebenes IT-Risikomanagement kann dann gewährleistet werden, wenn der Schritt von punktuell angesetzten Einzelbetrachtungen hin zu einem lebenden Prozess vollzogen wurde. Der Unterschied liegt darin, dass ein funktionierendes Risikomanagement an definierten Punkten in den Unternehmensprozessen automatisiert angestoßen wird. Wird ein Softwareprojekt gestartet, sollen Daten auf einem neuen Datenserver abgelegt werden, wird die Firewall ausgetauscht, geht ein Laptop verloren



oder wird ein Prozess zur Benutzeranlage erneuert – alle diese Beispiele berühren Teilbereiche des IT-Risikomanagements und müssten unter diesem Gesichtspunkt betrachtet und bewertet werden. Dies kann gelingen, wenn bei der Festlegung der Vorgehensweise für jedes dieser Beispiele von vornherein definiert wird, zu welchem Zeitpunkt welche Handlung mit Methoden des IT-Risikomanagements stattzufinden hat.

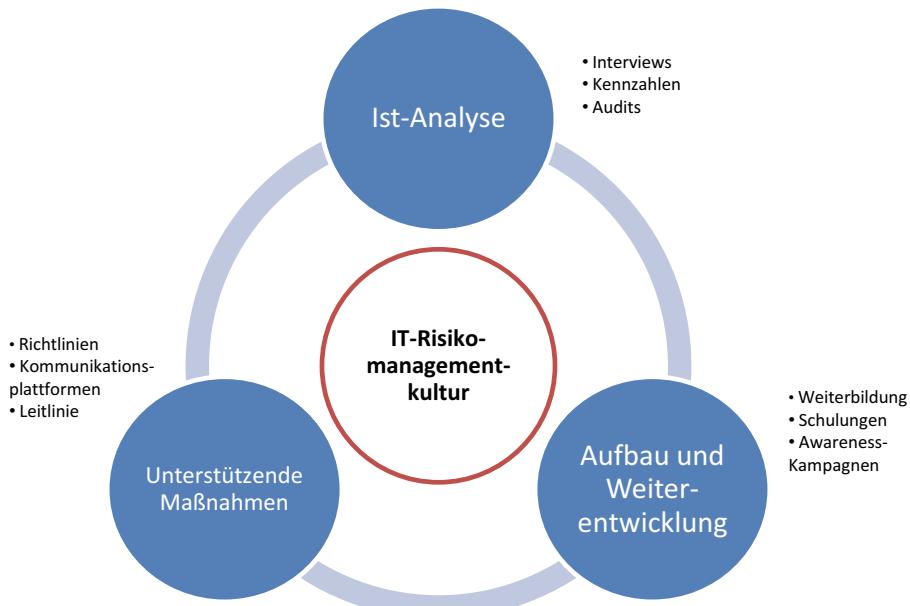


Abbildung 10.3: IT-Risikomanagementkultur

10

10.5 Operatives IT-Risikomanagement

Ein Risiko beschreibt ein Ereignis, das mit einer bestimmten Wahrscheinlichkeit eintritt und negative Auswirkungen hat. Im Schadensfall kann der Kreis der Betroffenen sehr klein sein, er kann aber auch jede einzelne mit dem Unternehmen verbundene Person beinhalten. Der Ausfall eines Steuerungsprogramms für Produktionsmaschinen betrifft zunächst die Produktionslinie, die nicht mehr arbeiten kann. Ist kein entsprechender Notfallprozess implementiert und dauert der Vorfall an, so kann der Fortbestand des Unternehmens gefährdet sein. Das Risikomanagement hat demzufolge die Aufgabe, Risiken beherrschbar zu machen und sicherzustellen, dass gesetzte



KAPITEL 10 – IT-RISIKOMANAGEMENT

Planwerte erreicht werden. Um dieser Vorgabe gerecht werden zu können, müssen alle relevanten Risiken bekannt sein, sie müssen in ihrer Tragweite eingeschätzt worden sein und es muss einen Plan geben, wie auf sie reagiert werden soll.

Hinweis

Ein grundsätzliches Problem bei der Einschätzung eines Risikos sind die in den meisten Fällen mathematisch nicht exakt zu bestimmenden Größen Eintrittswahrscheinlichkeit und der Schaden, den das Eintreffen eines Risikos verursachen würde.

10

Neben der strategischen Sicht sind weitere Perspektiven zu betrachten, um die operativen Risiken im Einzelfall hinreichend bewerten zu können. Dies geschieht, indem für jede Perspektive ein »Was wäre, wenn«-Szenario durchgespielt wird. Was wäre, wenn das Projekt mehr kostet, als im Budget eingeplant wurde, oder was wäre, wenn der Rollout einer neuen Software die Funktionsfähigkeit einer anderen Anwendung beeinträchtigen würde? Diese beiden Szenarien können jeweils einer anderen Risikokategorie zugeordnet werden und der langfristige, potenzielle Schaden für das Unternehmen kann jeweils unterschiedlich aussehen.



Abbildung 10.4: Verschiedene Risikoarten innerhalb eines Projekts



Die Beantwortung jeder dieser Fragen ist erforderlich, um das Projekt weiterbringen zu können. Daraus wird ersichtlich, dass ein großer Teil der Entscheidungen direkt auf dem Ergebnis einer Risikoanalyse beruht. Die im vorliegenden Kapitel beschriebenen Methoden sollen den Entscheider dabei unterstützen, diese Entscheidungen mithilfe eines formalen Prozesses zu treffen.

Innerhalb des IT-Security-Managements werden zunächst die folgenden Fragen im Mittelpunkt stehen:

- Welche Bedrohungen existieren für einen betrachteten Prozess oder de-taillierter für ein betrachtetes IT-System?
- Was wäre, wenn die Bedrohung einträfe? Welcher Schaden wäre zu erwarten?
- Wie wahrscheinlich ist es, dass diese Bedrohung auch wirklich eintritt?
- Wie kann ein Risiko, basierend auf den eben genannten Fragen, berechnet werden?

Die Antworten auf diese Fragen geben Auskunft über die Existenz und die Tragweite eines Risikos. Diese Informationen bestimmen im Folgenden den Rahmen für Maßnahmen, die getroffen werden müssen.

Wichtig

Eine Bedrohung (*threat*) kann ein Ereignis sein, durch das ein Schaden für das Unternehmen entstehen kann. Ist neben der Bedrohung auch eine ausnutzbare Schwachstelle vorhanden, dann spricht man von einer »Gefährdung« (*applied threat*). Zum Risiko (*risk*) wird eine Gefährdung dann, wenn es bereits hinsichtlich Eintrittswahrscheinlichkeit und potenziellem Schaden bewertet wurde. Bitte beachten: Im Englischen wird oft keine Unterscheidung zwischen Bedrohung und Gefährdung vorgenommen.

Die nachfolgende Vorgehensweise entspricht den Prozessmodellen, die in den ISO-Standards 31000 und 27005 normiert sind. Diese Standards dienen im Allgemeinen genauso auch den anderen Bereichen im Unternehmen, die ein Risikomanagement betreiben, als Grundlage und damit erleichtert es dem Manager IT-Security das Leben, wenn er sich im Sprachgebrauch und der Abfolge an diese Normen anpasst.



10.5.1 Vorgehensweise

Das IT-Risikomanagement beinhaltet folgende, grundlegende Schritte:

- die **Risikoidentifizierung** und die **Risikoanalyse**,
- die **Risikobewertung**
- und die **Risikobehandlung**.

Um diese Punkte abarbeiten zu können, ist einiges an Vorarbeit nötig, da zunächst die Rahmenbedingungen für das IT-Risikomanagement im Allgemeinen bestimmt werden müssen. Diese Rahmenbedingungen, die Festlegung des IT-Risikomanagementkontexts, beinhalten alle Aspekte, die im Vorfeld geklärt werden müssen. Dazu gehört die allgemeine IT-Risikomanagementrichtlinie mit Festlegungen des Aufgabenfelds des IT-Risikomanagements in Abgrenzung zum Unternehmensrisikomanagement und des Geltungsbereichs (*scope*). Der Geltungsbereich kann sich z.B. auf Unternehmenswerte beschränken, die die Kernprozesse des Unternehmens maßgeblich unterstützen, oder aber auch räumlicher Natur sein und nur das Rechenzentrum beinhalten.

10

Wichtig

Es ist wichtig, darauf zu achten, dass der Geltungsbereich sinnvoll und stringent gewählt wird. Es ist nicht sinnvoll, einen Großrechner dem Geltungsbereich zuzuordnen und die daran angeschlossenen Terminals außerhalb des Geltungsbereichs zu definieren. In diesem Fall ist das Risiko nicht eindeutig bestimmbar, und das Risikomanagement verliert an Bedeutung.

Einordnung des Risikos in den übergeordneten Kontext

- Risikoerfassung
 - Risikoanalyse
 - Risikoermittlung
 - Risikoabschätzung
 - Risikobewertung
- Risikobehandlung
- Kommunikation und fortlaufendes Monitoring



Abbildung 10.5: Phasen des IT-Risikomanagements



Des Weiteren muss darauf geachtet werden, dass die Anforderungen aus der IT-Compliance mit in diese Festlegungen einfließen. So kann die Risikovorsorge durch interne Regelungen, aber auch durch gesetzliche Anforderungen vorgeschrieben sein. Verträge mit Kunden und Lieferanten beinhalten häufig Klauseln, die verbindlich festlegen, wie mit Daten oder Produkten umzugehen ist. Alle umgesetzten Maßnahmen zur Erfüllung dieser Compliance-Anforderungen sollten auf einer Risikoanalyse basieren, die auch Punkte wie z.B. mögliche Regresszahlungen mit ins Kalkül ziehen.

Der innere Komplex, also der eigentliche Vorgang der Risikoerfassung und -behandlung, lässt sich mit den folgenden Schritten beschreiben, die in den folgenden Abschnitten näher ausgeführt werden:

1. Identifizierung und die Analyse von Risiken

- Innerhalb des Geltungsbereichs (*scope*) werden auf Basis von Daten aus dem Assetmanagement oder von einem Risikokatalog ausgehend die zu untersuchenden Unternehmenswerte (*assets*) wie IT-Systeme, Daten oder Software ermittelt.
- Für die zu untersuchenden Unternehmenswerte werden mögliche Bedrohungen und Schwachstellen identifiziert.
- Maßnahmen, die zur Reduzierung der Risiken bereits implementiert wurden, werden aufgenommen, da sie das Risiko vermindern können.
- Aus den nun vorliegenden Informationen wird unter Einbezug möglicher Auswirkungen auf den Geschäftsbetrieb durch Verlust von Vertraulichkeit, Verfügbarkeit oder Integrität der Werte ein Gesamtbild erstellt.
- Die Risikoanalyse setzt zudem einzelne Risiken in einen größeren Zusammenhang. Das kann Faktoren wie die allgemeine Risikotoleranz oder die Risikopolitik des Unternehmens beinhalten. Die Ergebnisse einer solchen Analyse können unter Umständen im nächsten Schritt zu einer anderen Bewertung führen.

2. Risikobewertung

- Für jedes identifizierte Risiko wird auf Basis aller gewonnenen Informationen eine Bewertung der Kritikalität vorgenommen. Dies kann z.B. unter Einbezug einer quantitativen Risikoermittlung stattfinden, wie sie im Abschnitt über Kennzahlen erläutert wird. Dabei wird das



Risiko anhand mathematischer Formeln errechnet. Zusätzlich wird das Risiko aus Sicht des Unternehmens betrachtet, um unabhängig von einer mathematischen Risikoberechnung ein möglichst realistisches Bild für die Auswirkungen des Eintretens des Risikos für den Betrieb zu bekommen.

- Abhängig von der Risikobewertung wird generell festgelegt, wie auf die einzelnen Risiken reagiert werden soll. Dazu findet grundsätzlich eine Entscheidungsfindung statt, wie das Risiko behandelt werden muss.

3. Risikobehandlung

- Anhand der Risikobewertung wird in diesem Prozessschritt entschieden, wie mit einem Risiko umgegangen werden soll.
- Auswahl der Maßnahmenziele und Maßnahmen, um auf die Risiken angemessen zu reagieren
- Ermittlung des Restrisikos für jedes Risiko nach Einführung von Maßnahmen
- Kommunikation des Restrisikos und Einholen der Zustimmung der Verantwortlichen, dass die vorgeschlagenen Restrisiken in dieser Form akzeptiert werden. Erfolgt diese Zustimmung nicht, so ist eine Reaktion darauf z.B. die Definition weiterer Maßnahmen, um das Risiko weiter zu reduzieren.

4. Dokumentation im Information-Security-Management-System (ISMS)

- Dokumentation des Risikomanagementvorgangs im ISMS. Zuordnung von Verantwortlichen und gegebenenfalls Einleitung von Workflows mit dem Ziel, die definierten Maßnahmen umzusetzen.

10.5.2 IT-Risikomanagementprozess

Im Rahmen des IT-Security-Managements wird die Betrachtung von Risiken in Bezug auf einen Unternehmenswert oder einen Prozess in den seltensten Fällen ein einmaliger Vorgang bleiben. Selbst in den Fällen, in denen das aufgedeckte Risiko an einen Dienstleister ausgelagert bzw. von einem Dritten versichert wird, bleibt die Frage nicht aus, ob das Risiko nach Ablauf einer Zeitspanne oder nach technischen Veränderungen noch existiert, ob es größer geworden ist und ob die Risikobehandlung noch adäquat ist.

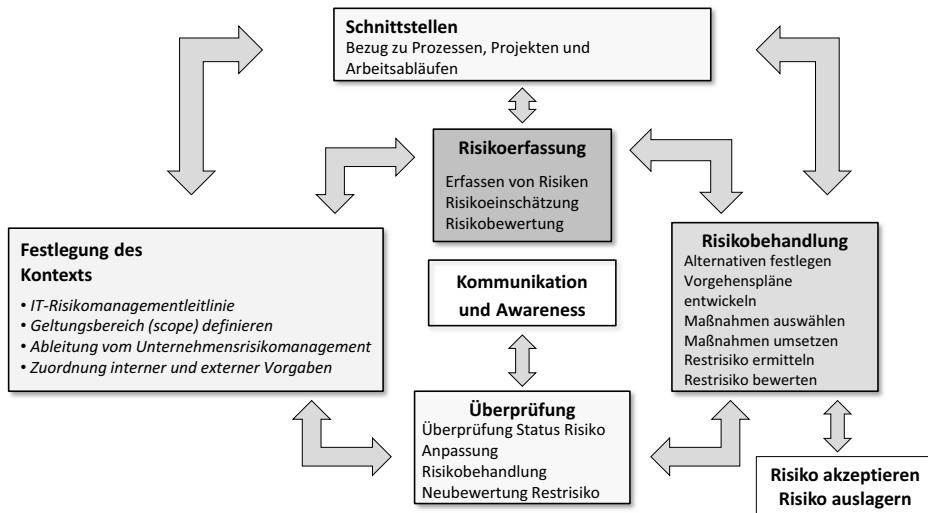


Abbildung 10.6: Abhängigkeiten verschiedener Phasen des IT-Risikomanagements

10

Risiken und die von einem Schadensereignis betroffenen Unternehmenswerte müssen, um zu einer ganzheitlichen Betrachtung gelangen zu können, in einen funktionalen Zusammenhang gebracht werden. Dieser Zusammenhang wird als »Kontext« bezeichnet.

Risiken hängen direkt von Schwachstellen, Bedrohungen und der Bedeutung des zugrunde liegenden Werts ab. Veränderungen an diesen Parametern bedingen oft auch eine Neubewertung. Um diese wiederholt, formal und nachvollziehbar gestalten zu können, wird ein Prozess benötigt, der diesen Vorgang vorantreibt. Dieser kontinuierliche Verbesserungsprozess kümmert sich um die Identifizierung, Analyse, Bewertung und Behandlung von Risiken, hilft bei der Festlegung von Maßnahmen und kontrolliert deren Umsetzung. Innerhalb dieses Prozesses kann das Restrisiko einer ständigen Änderung unterworfen sein. Überschreitet es bei einer erneuten Prüfung einen vordefinierten Grenzwert, so kann die Festlegung neuer Maßnahmen erforderlich werden.

Hinweis

Ein weiteres Kriterium für einen funktionierenden Prozess ist die gelebte Konsequenz. IT-Risiken zu erfassen und Maßnahmen zu definieren, ist nur dann sinnvoll, wenn dieser Vorgang in allen Bereichen mit gleicher



Stringenz verfolgt wird. Unterliegen Maßnahmen, die ein IT-Bereich einführen muss, automatisch höherer oder auch niedriger Priorität im Vergleich zu einer Maßnahme in einem Fachbereich, dann verliert der Gesamtprozess an Glaubwürdigkeit und Verlässlichkeit.

10

Betroffene eines IT-Risikos sind, wie oben bereits erwähnt, unter Umständen alle mit dem Unternehmen verbundenen Personen. In vielen Fällen betrifft es aber auch nur einen Arbeitnehmer. Aus dem Ausfall dieser einen Tätigkeit können sich wiederum weitere, neue Risiken für andere Personen und andere Prozesse ergeben. Daraus ist leicht zu erkennen, dass selbst scheinbar einzeln auftretende Risiken nicht singulär betrachtet werden können. Es ist immer auch eine Betrachtung des Umfelds erforderlich, um die jeweilige Tragweite einschätzen zu können.

10.5.3 Übergeordnete Risikobetrachtung

Ein Risiko ist nicht per se vorhanden. Zu seiner Entstehung sind ein Initiator, der den Eintritt auslöst, und die Möglichkeit, dass es überhaupt ausgelöst werden kann, erforderlich. Die Höhe des Risikos für ein bestimmtes Zielobjekt wiederum wird durch eine Reihe weiterer Faktoren bestimmt. Parameter wie Schwachstellen, Eintrittswahrscheinlichkeit und möglicher Schaden sind, jeder für sich gesehen, wichtig, um der Kritikalität angemessene Maßnahmen bestimmen zu können. Die verschiedenen Ausprägungen dieser Parameter zu kennen, ist zudem entscheidend für die Ist-Aufnahme und die Analyse des Risikos. Geht man bei der Erfassung dieser Faktoren strukturiert vor, so bildet dies den roten Faden, der für das Risikomanagement erforderlich ist. Außerdem können Risiken auf dieser Basis leichter geordnet und klassifiziert werden.

Alle Handlungen in einem Unternehmen sind mit operativen Risiken verbunden. Sie ergänzen auf vielfältige Weise die strategischen Risiken wie das Marktrisiko oder das Kreditrisiko von Banken und Versicherungen. Ein universelles IT-Risikomanagement ist also nur möglich, wenn operative und strategische Risiken mit in die Überlegungen eingebunden werden. So kann das operative Risiko eines Druckerausfalls nur dann adäquat eingeschätzt werden, wenn auch die strategischen Folgen bekannt sind. Ein Drucker, der Warenausgangsetiketten druckt, kann die Auslieferung verzögern und damit



einen Schaden anrichten, der weit über den Horizont der IT hinausgeht. Falls die Unternehmenswebsite gehackt und mit diskriminierenden Äußerungen verunstaltet wird, dann ist neben den rein betriebswirtschaftlichen Folgen auch an die Folgen für das Ansehen des Unternehmens in der Außenwirkung zu denken. Dazu kommen strafrechtliche Konsequenzen, die schnell in den Zuständigkeitsbereich des Unternehmensrisikomanagements fallen können.

Die Bandbreite operativer Risiken ist sehr groß und komplex, und häufig sind Risiken miteinander verbunden und voneinander abhängig. Ein Teil davon ist zudem spezifisch für jedes Unternehmen und kann nicht ohne Weiteres aus vorbereiteten Listen übernommen werden. Dies macht das Fachgebiet so komplex und bietet weitere Gründe, die für ein streng formales Vorgehen bei der Durchführung eines Risikomanagements sprechen. Fällt der bereits erwähnte Drucker aus, dann hat dies Folgen für die Warenauslieferung. Vielleicht entsteht aber auch auf dem dafür zuständigen Druckserver ein schnell wachsender Stau an nicht druckbaren Druckaufträgen, die irgendwann zum Ausfall dieses Servers führen, da die Platten voll sind. Da auf dem Druckserver noch andere kritische Drucker angeschlossen sind, zeigt sich dann schnell, dass hier zwei oder noch mehr operative Risiken eng miteinander verknüpft sind. Eine strukturierte Vorgehensweise wird in diesem Fall so ablaufen, dass zunächst der Druckserver und dann alle angeschlossenen Drucker einzeln betrachtet werden.

Hinweis

Es existiert eine Reihe von Ansätzen, um für ein Unternehmen Risikoarten zu definieren. Ihnen allen gemeinsam ist der Wunsch, dass Risiken in irgendeiner Weise kategorisiert werden sollten. Auf diese Art wird sowohl die strukturierte Vorgehensweise bei der Risikoerfassung unterstützt als auch die Möglichkeit eröffnet, statistische Aussagen nach Häufigkeiten etc. treffen zu können.

Die Gliederung in Risikoarten hat eine weitere wichtige Aufgabe. Von ihr ausgehend kann für jede Art an Risikokategorie eine generische Liste möglicher Bedrohungen erstellt werden, auf die im Rahmen des IT-Risikomanagements zurückgegriffen werden kann. Dadurch wird es möglich, das IT-Risikomanagement weiter zu formalisieren und zu automatisieren.



Risiken bezogen auf Schutzziele

Konzentriert man sich auf die grundlegenden Aufgaben der IT-Security, so beziehen sich Risiken in erster Linie auf eine Reihe von Schutzz Zielen, von denen die am häufigsten genutzten den Schutz von Vertraulichkeit, Verfügbarkeit und Integrität betreffen. Bedrohungen sollten sich in eine oder mehrere dieser Kategorien einordnen lassen. Ist dies nicht möglich, so kann diese Problematik durch die Definition weiterer Schutzz Zielen aufgelöst werden.

Bedrohungen, die im Kontext von Schutzz Zielen aufgeführt werden, beziehen sich hauptsächlich auf IT-Systeme und Einrichtungen, also auf Risiken im generellen Kontext der IT. Sollen Risiken für immaterielle Dinge wie z.B. der Imageschaden für ein Unternehmen eingeschätzt werden, so kann kein direkter Bezug zu den eben genannten Schutzz Zielen hergestellt werden. In diesem Fall ist wiederum der Umweg über entsprechende IT-Systeme zu gehen. Wird also eine problematische Nachricht auf dem öffentlichen Webserver propagiert, so stellt sich dieser Webserver als das IT-System dar, das das Risiko darstellt, und die Bedrohung fällt damit in die Zuständigkeit des Schutzz Ziels »Integrität«. Die Einschätzung eines möglichen Schadens wird in diesem Fall auf strategischer Ebene geschehen müssen.

10

Integrität	<ul style="list-style-type: none"> • Übernahme Datenbank • Falsche Benutzereingabe • Fehlerhafte Datenverarbeitung • Schadsoftware • ...
Verfügbarkeit	<ul style="list-style-type: none"> • Ausfall Backup/Restore • Ausfall Netzwerk • Ausfall zentrale Server • Schadsoftware • Denial-of-Service-Angriff • ...
Vertraulichkeit	<ul style="list-style-type: none"> • Übernahme Datenbank • Diebstahl von Daten • Brute-Force-Angriff auf Passwörter • ...

Abbildung 10.7: Risiken bezogen auf Schutzz Zielen

Ein Blick auf Abbildung 10.7 macht deutlich, dass sich Schutzz Zielen nicht vollständig voneinander abgrenzen lassen. Es tauchen immer wieder Risiken auf,



die mehr als einem Schutzziel zugeordnet werden können. Eine Schadsoftware kann auf einem Datenserver sehr wohl sowohl die Integrität der Daten als auch die Vertraulichkeit oder Verfügbarkeit gefährden. Aus diesem Grund ist als Risikoart jeweils das Schutzziel als auch das konkrete Risikoszenario anzugeben.

Risiken bezogen auf unabhängige Risikoarten

Ein weiterer Ansatz verfolgt die Erstellung einer generellen Liste von Risikoarten, die sich über verschiedene Risikobereiche erstrecken. Eine solche Liste könnte mit dem Ansatz der Ableitung aus den Schutzz Zielen kombiniert werden. Mögliche Risikoarten wären in diesem Fall beispielhaft die Arten:

- IT-technisches Risiko
- Prozessrisiko
- Softwarerisiko
- Menschliches Risiko
- Organisatorisches Risiko
- IT-Compliance-Risiko
- Dienstleister
- Betriebsrisiko

10

Die aufgeführten Risikoarten sind im Gegensatz zu denen, die an allgemeinen Schutzz Zielen ausgerichtet sind, vom Geschäftszweck eines Unternehmens abhängig. Ein produzierendes Unternehmen wird ein »Produktionsrisiko« und ein »Lieferrisiko« anführen, während eine Bank von einem »Marktrisiko« oder einem »Kreditrisiko« spricht. Darin liegt sowohl die Stärke als auch die Schwäche dieser Definition. Die stärkere Spezialisierung führt zu einem mehr angepassten Risikomanagement, eine an Schutzz Zielen orientierte Vorgehensweise zu einer besseren Vergleichbarkeit mit anderen Unternehmen.

10.5.4 Schwachstellen

Jedes System hat Schwachstellen. Je komplexer ein System ist, desto mehr Schwachstellen sind potenziell vorhanden. IT-Systeme gehören in die Kategorie »komplexe Systeme« und beherbergen bereits entdeckte und noch nicht bekannte Schwachstellen. Gerade die noch nicht gefundenen Schwachstellen beinhalten das Risiko, dass die Person, die sie aufdeckt, diese auch ausnutzen



kann und wird, ohne dass es zu diesem Zeitpunkt Abwehrmechanismen gibt. Insbesondere bei neu entwickelten Viren, Würmern und Trojanern ist der sogenannte »Zero Day Attack« möglich, also ein Angriff zu einem Zeitpunkt, zu dem Hersteller von Antivirensoftware noch keine entsprechenden Viren-pattern veröffentlicht haben.

Wichtig

Schwachstellen machen IT-Systeme nicht nur gegen den absichtlichen oder unabsichtlichen Angriff durch Personen verwundbar. Schwachstellen in einer kritischen Software können auch durch ein Schnittstellenprogramm oder durch die Eingabe bestimmter Daten zu einer Bedrohung führen. Diese Tatsache muss bei jeder Risikoanalyse mitbetrachtet werden.

10

Eine Auflistung bekannter Schwachstellen und einige diesbezügliche Statistiken können unter <http://www.sans.org> abgerufen werden. Das »sysAdmin, Audit, Network, Security Institute« (SANS) wurde 1989 gegründet und verfolgt das Ziel, Sicherheitslecks zu veröffentlichen, den Erfahrungsaustausch zu fördern und gemeinsam Lösungen zu entwickeln. Sowohl staatliche als auch private Stellen arbeiten hier zusammen, um die Datenbestände aktuell zu halten.

Bei der Auflistung von Schwachstellen wird zwischen logischen und physischen Schwachstellen unterschieden.

Zu den **logischen Schwachstellen** gehören:

- Mangelhafte Schulung des Bedienpersonals: Dabei ist es unerheblich, ob es sich um Programmierer, Anwender oder Hardwarebetreuer handelt. Der Mensch ist eine Schwachstelle, und mangelhafte Einarbeitung, Schulung oder nicht vermitteltes Sicherheitsbewusstsein führt in vielen Fällen zum Eintritt eines Schadens.
- Softwarefehler in Betriebssystemen oder in Anwendungsprogrammen: Je komplexer und umfangreicher Installationen werden, desto mehr potenzielle Sicherheitslöcher sind vorhanden. Vor allem Applikationen, die über das Internet kommunizieren, sind stark gefährdet, was sich im medialen Interesse widerspiegelt. Nicht zu Unrecht denkt man dabei zunächst an



Webbrowser und E-Mail-Clients und danach an Apps auf dem Mobiltelefon oder die Datenübertragung in Cloud-Speicher. Alle diese Applikationen sind dafür ausgelegt, die lokale Netzwerkumgebung zu verlassen, und öffnen sich damit einer Reihe von unkontrollierbar arbeitenden Angreifern. In der Top-20-Liste von SANS sind diese Schwachstellen auf den vorderen Plätzen zu finden.

- Bruch mit der Regel, nur die Komponenten von Applikationen oder Betriebssystemen zu installieren, die für die Erfüllung der gestellten Anforderungen erforderlich sind. Dabei kann es sich um Module von Software handeln, die nicht benötigt werden und Sicherheitslücken beinhalten, oder aber auch um Systemprogramme auf Betriebssystemebene, die unbeachtet und nicht gewartet Fehler beinhalten. Das Risiko steigt insbesondere dann an, wenn die eben genannten Systemprogramme über offene Ports über das Netzwerk kommunizieren können.
- Die Authentifizierung von Benutzern ist über das Internet vielen Gefahren ausgesetzt. Diese reichen von Phishing-Angriffen bis hin zu Brute-Force-Angriffen auf User-Passwort-Kombinationen. Aber auch innerhalb des Unternehmens ist es wichtig, starke Passwörter zu nutzen, und gleichzeitig durch Schulungsmaßnahmen zu verhindern, dass diese unter Tastaturen geklebt werden.
- Ein weiteres wichtiges Feld ist das der Verschlüsselung. Sollte es eigentlich selbstverständlich sein, dass Geschäftskorrespondenz ausschließlich verschlüsselt per E-Mail versandt wird, so ist dies noch immer kein Standard. Das Gleiche gilt für hochsensible Daten, die unverschlüsselt auf Datenservern abgelegt werden. Auch mobile Endgeräte zählen dazu und nehmen einen wichtigen Platz auf der SANS-Liste der Zukunftsrisiken ein. Jedes Gerät, das gestohlen oder verloren werden kann und das Daten enthält, sollte diese nur verschlüsselt gespeichert haben. Zu den üblichen Verdächtigen zählen Laptops, Mobiltelefone, Kameras, Tablets, Fitness-Armbänder mit gespeicherten, personenbezogenen Daten, MP3-Spieler und alle anderen Geräte, auf denen Daten abgelegt werden können. Neben den gespeicherten Daten ist auch der Transportweg der übermittelten Daten zu beachten. Dabei geht es um Daten, die über Leitungen übertragen werden, um Daten, die über Wireless LAN oder per Mobilfunk übertragen werden, und um Sprache, die mittels Voice-over-IP übermittelt wird. In allen diesen Fällen ist es sinnvoll, über Verschlüsselungsmöglichkeiten nachzudenken.



- Fehlende, unvollständige oder falsche Dokumentationen sind eine Schwachstelle, die den Betrieb oder die Wiederinbetriebnahme eines Systems verzögern oder verhindern können.

Zu den logischen Schwachstellen kommt eine Reihe von **physischen Schwachstellen** hinzu. Dabei handelt es sich um systemimmanente Schwachstellen, die bei Versagen den Ausfall des Systems verursachen können. Dazu gehören unter anderem:

- Betriebsvoraussetzungen wie Strom und eine gekühlte Umgebungstemperatur. Dadurch verlagern sich sehr oft die Schwachstellen weg vom eigentlichen IT-System hin zu Infrastrukturkomponenten wie der Klimaanlage und dem Sicherungskasten oder dem Notstromaggregat.
- Gesicherte und überwachte Räumlichkeiten sichern Systeme vor Diebstahl oder Sabotage. Die Sicherheit beginnt dabei schon bei der Auswahl des Lieferanten durch den Einkauf und die Sicherstellung, dass z.B. Telefonapparate, die in sensiblen Bereichen eingesetzt werden sollen, ohne Abhöreinrichtungen ausgeliefert werden.

10

10.5.5 Bedrohungen

Eine Gefährdung liegt dann vor, wenn eine Bedrohung und eine Schwachstelle vorhanden ist und eine Möglichkeit existiert, diese auszunutzen. Die Bedrohung ist damit die allgewärtige Gefahr, dass ein Schutzziel verletzt wird. Da es nicht immer bekannt ist, ob neben der Bedrohung auch eine Schwachstelle vorhanden ist, geht man häufig dazu über, dies schlicht vorauszusetzen und die Bedrohung damit automatisch in den Rang einer Gefährdung zu erhöhen. In den folgenden Abschnitten folgen wir diesem Trend und schreiben grundsätzlich von einer Bedrohung und differenzieren nicht zwischen Gefährdung und Bedrohung.

Ein IT-System mit einer Sicherheitslücke im Betriebssystem ist so lange keine Bedrohung, solange kein Weg für einen Angreifer existiert, diese Lücke auszunutzen. Die Möglichkeit zum Angriff und der Weg, den ein Angreifer nehmen könnte, wird »Angriffspfad« genannt. Ein Angriffspfad liegt zumeist erst dann vor, wenn mehrere Bedingungen erfüllt sind. So kann ein Angriff auf ein Betriebssystem z.B. erst dann stattfinden, wenn der Rechner vernetzt ist, wenn der Angreifer in das Netz kommt und wenn ein bestimmtes Betriebssystem in einer definierten Version installiert ist. Zusammengefasst



lässt sich also sagen, dass eine Bedrohung vorliegt, wenn mindestens eine Schwachstelle und mindestens ein passender Angriffspfad existieren.

Wichtig

Für das IT-Security-Management und das IT-Risikomanagement bedeutet dies, dass alle Angriffspfade für alle Schwachstellen ausgeschlossen werden müssen, um alle Bedrohungen für einen Unternehmenswert zu eliminieren.

Die nachfolgende Gliederung von Bedrohungen stellt eine exemplarische Aufstellung dar:

■ Technik

Die Technik umfasst alle IT-Systeme, die Daten verarbeiten. Ein Ausfall eines Systems führt zu verringrigerer Verfügbarkeit. Fehler in der Verarbeitung, z.B. aufgrund fehlerhafter Applikationen, kann zu Integritätsverlust, Verlust der Vertraulichkeit oder zur Nichtverfügbarkeit der Daten führen.

■ Organisation

Ist die Zuständigkeit von Organisationseinheiten innerhalb des Unternehmens nicht klar definiert, so können Angriffe begünstigt und deren Erkennung und Aufklärung erschwert werden. Maßnahmen aus den Bereichen Informationsschutz, Organisation und Richtlinien zielen auf die Reduzierung des Bedrohungspotenzials, das dadurch geschaffen wird. In diese Sparte fallen auch Bedrohungen, die sich aus Firmenzusammenschlüssen oder durch die Anbindung externer Dienstleister ergeben.

■ Mensch

Menschliches Versagen, Sabotage oder gezielte Angriffe gehören in diese Kategorie genauso wie die Anfälligkeit für Social-Engineering-Angriffe gegen Mitarbeiter. Aus diesen Gründen sind Gegenmaßnahmen in den Bereichen Schulung der Mitarbeiter und Verwaltung von Rechtestrukturen zu suchen.

■ Infrastruktur

In diese Rubrik fallen Bedrohungen wie der Ausfall von Klimageräten im Rechenzentrum, der Ausfall von Strom, aber auch Bedrohungen durch Einbruch, Feuer, Wasser, Unwetter oder Erdbeben.



Die Aufgabe von Maßnahmen ist es, die Bedrohung als solche oder deren Eintrittswahrscheinlichkeit zu reduzieren. Werden keine Maßnahmen installiert, so bleibt die Bedrohung akut oder der Grad der Bedrohung steigt sogar an, und wir sprechen von einer unbehandelten Schwachstelle.

Hinweis

Bedrohungen beziehen sich immer auf ein Zielobjekt. So kann z.B. ein Bezug der Bedrohung »Feuer« auf das Zielobjekt »Gebäude Rechenzentrum« hergestellt werden.

10

Neben der Einordnung nach technischen Kriterien können Bedrohungen auch nach der Art der Initiierung gegliedert werden. Auf oberster Ebene unterscheidet man zwischen vorsätzlichen Bedrohungen und zufälligen Bedrohungen. Vorsätzliche Bedrohungen werden durch Menschen ausgelöst, und es besteht grundsätzlich die Problematik, dass implementierte Maßnahmen vom Angreifer analysiert und anschließend umgangen werden. Der Initiator Mensch zählt deshalb zu den flexiblen Auslösern, und hierbei werden deutlich höhere Aufwände in die erneute Überprüfung bzw. das Monitoring gesteckt werden müssen. Zu den zufälligen oder ungelenkten Bedrohungen zählen natürliche Ereignisse wie Naturkatastrophen oder Hardwarefehler, aber auch durch Menschen hervorgerufene, unabsichtliche Fehler.

10.5.6 Zusammenspiel von Bedrohungen, Schwachstellen und Maßnahmen

Ein Risiko berechnet sich durch die Bewertung der Faktoren Bedrohung, Schwachstelle und implementierte Maßnahmen mit den Stellgrößen Eintrittswahrscheinlichkeit und potenziellem Schaden. Alle drei Faktoren stehen wiederum in Verbindung mit dem technischen Umfeld, dem Unternehmenszweck, der Risikoaffinität der Kollegen und vielen anderen Variablen. Ein Risiko, das sich aus diesen drei Faktoren zusammensetzt, kann also von Unternehmen zu Unternehmen unterschiedlich bewertet werden. Das Gleiche gilt für die Maßnahmen, die zur Reduzierung eines Risikos ausgewählt und implementiert werden. Es gibt auch hierfür keine allgemeingültige Vorgehensweise. Ist es für eine Bank selbstverständlich, den Zugang zum eige-



nen Großrechner aufwendig zu schützen, so kann dies bei einem Unternehmen, das alle Daten in einem Cloud-Speicher liegen hat, zweitrangig sein.

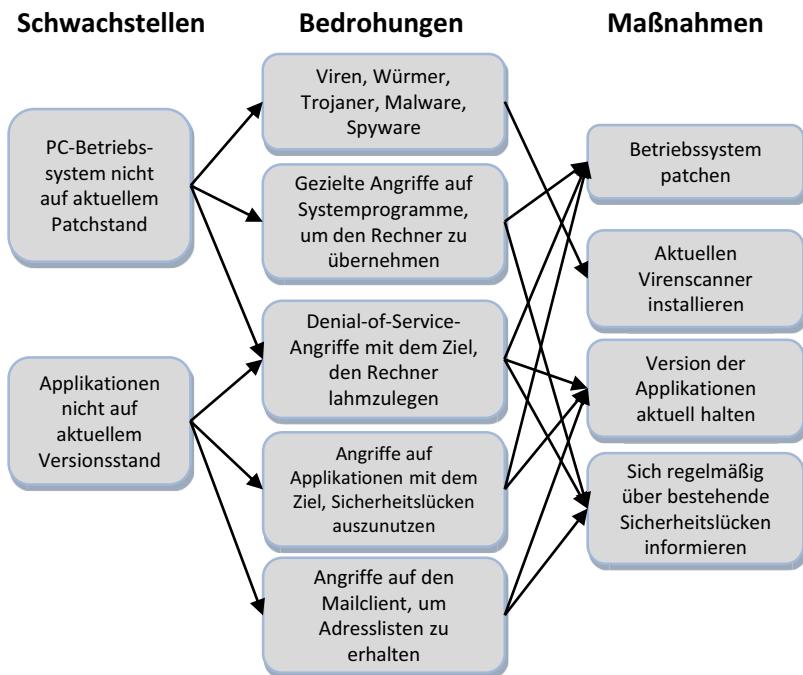


Abbildung 10.8: Zusammenhang von Schwachstellen, Bedrohungen und abgeleiteten Maßnahmen

In Abbildung 10.8 ist zu erkennen, dass es sich sowohl bei der Beziehung zwischen Schwachstelle und Bedrohung um eine *m:n*-Beziehung handelt als auch bei der Beziehung zwischen Bedrohung und Maßnahme. Daraus kann man mehrere Schlussfolgerungen ziehen:

- Es ist wichtig, die ermittelten Schwachstellen, Bedrohungen und die daraus resultierenden Maßnahmen zu dokumentieren und anschaulich zu machen. Die Gefahr ist groß, aufgrund der vielfältigen Abhängigkeiten den Überblick zu verlieren. Das liegt auch daran, dass die Zielgruppe für eine Darstellung aus dem IT-Risikomanagement unter Umständen eine andere ist als diejenige, die für den Betrieb verantwortlich ist.
- Aus Sicht der Maßnahmen gesehen kann mit einer Maßnahme oft eine ganze Reihe von Bedrohungen und Schwachstellen adressiert werden. Ein



gutes Beispiel ist das Patchmanagement. Einmal als Maßnahme definiert und dokumentiert, lässt sie sich auf beinahe jedes IT-System direkt anwenden. Dabei werden immer die gleichen Bedrohungen und Schwachstellen adressiert. Mittels einer Reihe von wenigen Standardmaßnahmen können so häufig ein Großteil der Bedrohungen und Schwachstellen abgedeckt werden. Dies wird aber erst dann auf einen Blick ersichtlich, wenn eine Darstellung der Abhängigkeiten vorliegt.

- Der Einsatz geeigneter Software zur Darstellung von Risiken und der Zusammenhänge der verschiedenen Risikoparameter ist sinnvoll, um zum einen den Überblick zu behalten und zum anderen, um Berichte für die verschiedenen Ebenen von Adressaten generieren zu können. Außerdem lässt sich so die Entwicklung der Risiken über die Zeit nachvollziehen.

10

10.5.7 Verhältnismäßigkeit

Die vielen Parameter, die in den Disziplinen Schwachstellenanalyse, Eintrittswahrscheinlichkeit und Kosten definiert werden können, täuschen darüber hinweg, dass eine mathematisch vollständige und korrekte Beurteilung eines Risikos und die Auswirkungen von Maßnahmen nicht möglich sind. Weitere Einschränkungen kommen hinzu, da es nicht möglich ist, in jedem Fall jedes Risiko aus allen erforderlichen Perspektiven zu betrachten. Das liegt vor allem am Aufwand, der zu treiben wäre, wenn Risiken eingeschätzt werden sollen, die jeden Teilbereich eines Unternehmens mehr oder weniger stark betreffen. Dazu kommt, dass die Schwere eines Risikos auch vom Parameter Zeit abhängig ist, der sich in einer Analyse nur schwer nachvollziehen lässt. So steigt das Risiko, dass ein elektronisch abgelegtes Firmengeheimnis offenbart wird, mit der Anzahl an Geheimnisträgern genauso wie mit dem steigenden technischen Fortschritt der Angreifer und damit häufig mit der Zeit.

Diese Schwierigkeiten betreffen alle Formen des unternehmerischen Risikomanagements, und aus diesem Grund sollte zu Beginn einer Risikobetrachtung die Frage nach der Verhältnismäßigkeit gestellt werden. Ist es angemessen, den Prozess der Risikoeinschätzung zu starten? Ist es angemessen, Maßnahmen zu implementieren? Ist es angemessen, ein Risiko weniger als einmal pro Monat neu zu bewerten? Je nach Antwort in den verschiedenen Stadien eines Risikomanagements wird sich auch die generelle Vorgehensweise verändern. Zudem muss allen Beteiligten immer wieder deutlich gemacht werden, dass es keine vollständige Sicherheit gibt und – noch wichtiger – dass es keine Garantie gegen zukünftige Entwicklungen gibt.



tiger – dass es häufig unangemessen ist, für die letzten Prozenten der Restrisikominimierung horrende Summen für zusätzliche Maßnahmen zu investieren.

10.6 Schutzbedarfsfeststellung

Unternehmenswerte müssen geschützt werden. Aber nicht jeder Unternehmenswert ist mit jedem anderen Unternehmenswert gleichzusetzen. Jede Spielart an Werten ist denkbar und auch eine Vielzahl an Einstufungen, was deren Wichtigkeit betrifft. Um eine Entscheidung treffen zu können, ob ein Wert aus der Sicherheitsperspektive betrachtet wird und mit welchem Aufwand dies geschehen soll, hängt primär von dessen Wichtigkeit ab. Um die Entscheidung nicht aus dem Bauch heraus treffen zu müssen und um Nachvollziehbarkeit sowie Transparenz zu schaffen, gibt es die Schutzbedarfsfeststellung. Ziel ist hierbei, sowohl Kriterien für die Feststellung von Wichtigkeit als auch eine formale Vorgehensweise bei deren Festlegung anzubieten.

10

10.6.1 Schutzziele

Die Grundlage für die Schutzbedarfsfeststellung sind die Grundwerte der IT-Security: Vertraulichkeit, Integrität und Verfügbarkeit. Im Englischen heißen diese Begriffe *confidentiality*, *integrity* und *availability* und werden üblicherweise mit »CIA« abgekürzt.

Abhängig von Geschäftszweck und den betrachteten Kernprozessen können eine Reihe weiterer Schutzziele vereinbart werden. Dabei kann man zwischen alleinstehenden und abhängigen Schutzzieilen unterscheiden. Die oben genannten Schutzziele gehören zu den alleinstehenden. Ein vierter alleinstehendes Schutzziel ist das der Verbindlichkeit. Dabei kann der Sender darauf vertrauen, dass der Empfänger derjenige ist, der er vorgibt zu sein, und andersherum. Abhängige Schutzziele wären z.B. Effektivität, IT-Compliance, Datenschutz oder Qualität. Diese Schutzziele basieren im Wesentlichen auf einem oder auf mehreren alleinstehenden Schutzzieilen. So ist beispielsweise für die Sicherstellung von Qualität sowohl das Erreichen einer definierten Verfügbarkeit als auch eines fehlerfreien Ergebnisses (Integrität) erforderlich.

Bezogen auf diese Grundwerte werden im Rahmen der Schutzbedarfsfeststellung Unternehmenswerte klassifiziert. Im Grunde bedeutet das, dass Werte



hinsichtlich der Schutzziele bewertet werden, indem Fragen wie »Wie wichtig ist Vertraulichkeit für den Wert DATENSERVER01?« oder »Wie wichtig ist die Verfügbarkeit von IT-System PC002?« beantwortet werden.

Vertraulichkeit

Informationen werden häufig nur einem eingeschränkten Personenkreis zugänglich gemacht. Dies zu gewährleisten, ist die Aufgabe des Schutzzieles Vertraulichkeit, im Englischen *confidentiality* genannt. Dabei ist der gesamte Life-cycle einer Information zu betrachten. Informationen in Form von Daten müssen deshalb von der Entstehung über die Übertragung über Datennetze und die Speicherung bis hin zur Datensicherung gesteuert werden. Im Laufe des Daten-Lifecycles können unterschiedliche Methoden zur Sicherung der Vertraulichkeit zum Einsatz kommen. Diese reichen von der Verschlüsselung bis hin zur User-Passwort-Kombination beim Zugriff auf ein Backup der Daten.

10

Verfügbarkeit

Die Verfügbarkeit von Dienstleistungen, die durch die Informationstechnologie bereitgestellt werden, auf Englisch *availability*, beschreibt das Verhältnis zwischen dem vereinbarten Zeitraum der Verfügbarkeit und den tatsächlich eingehaltenen Zeiten. Maßnahmen aus dem Bereich des Verfügbarkeitsmanagements, das einen Bereich des IT Business Continuity Managements darstellt, dienen der Steigerung der Verfügbarkeit von IT-Systemen und -Prozessen.

Integrität

Wird die Integrität, auf Englisch *integrity*, erhalten, so wird dafür Sorge getragen, dass Informationen nur von berechtigten Personen in beabsichtigter Weise verändert werden. Integrität liegt z.B. vor, wenn Daten unverändert von einem Sender zu einem Empfänger übermittelt werden. Ein Beispiel ist die Übermittlung von Transaktionen auf Konten bei verschiedenen Banken. Es ist entscheidend, dass die ursprünglich eingegebenen Daten denen entsprechen, die beim Zielkonto ankommen. Integrität kann dabei sowohl die Fälschungssicherheit als auch den Datenverlust ansprechen. Die Entscheidung, ob Integrität gewahrt wurde, wird zwar binär beantwortet: Es wurden Daten verändert oder nicht. Im täglichen Umgang kann Art und Umfang von Änderungen sehr wohl den Aufwand beeinflussen, der in die Bereinigung der Informationen investiert werden muss.



Authentizität

Die Authentizität einer Information stellt sicher, dass ein Sender eindeutig einer Information zugeordnet werden kann. Das Wort stammt aus dem Lateinischen und bedeutet so viel wie »echt« oder »verbürgt«. Technisch wird dies z.B. durch die Einführung einer digitalen Signatur gelöst. Dabei unterschreibt der Sender die Nachricht unter Zuhilfenahme einer mittels PGP verschlüsselten Signatur, die ausschließlich der Sender nutzen kann. Auf der anderen Seite kann der Empfänger mithilfe des öffentlichen Teils des Schlüssels überprüfen, ob die digitale Signatur echt ist. Werden solcherart Signaturen nicht eingesetzt, so zählen Man-In-The-Middle-Angriffe als häufig gebrauchtes Angriffsmittel, Datenverkehr während der Übermittlungsphase abzufangen, umzuleiten, zu verändern und dann dem Empfänger wieder unterzuschieben.

10

Im Gegensatz zu den am häufigsten verwendeten Schutzz Zielen Vertraulichkeit, Verfügbarkeit und Integrität wird die Authentizität innerhalb von Unternehmen seltener betrachtet. Deshalb ist sie häufig kein Bestandteil von Klassifizierungsrichtlinien. Bei einer Entscheidung, welche Schutzz Zielen betrachtet werden sollen, wird es aber vor allem auf den Geschäftszweck des Unternehmens ankommen. In Banken und Versicherungen wird sich deshalb sehr viel häufiger das Schutzz Ziel Authentizität finden als in Produktionsbetrieben. Mit der weiteren Zunahme von Angriffen, die darauf zielen, durch das Vortäuschen von Rechnungen oder Anweisungen Geld zu erschleichen, wie es z.B. typisch für den »CEO-Fraud« genannten Angriff ist, wird auch das Schutzz Ziel an Bedeutung gewinnen.

Nichtabstreitbarkeit

Die Nichtabstreitbarkeit, auf Englisch *non-repudiation*, bezeichnet die Sicherstellung, dass der Empfang bzw. das Senden einer Information nachträglich nicht bestritten werden kann, da technische Möglichkeiten vorliegen, beides nachzuweisen.

Es wird dabei unterschieden zwischen:

- Nichtabstreitbarkeit der Herkunft: Der Absender einer Nachricht kann den Versand nachträglich nicht bestreiten.
- Nichtabstreitbarkeit des Erhalts: Der Empfänger einer Nachricht kann den Empfang nachträglich nicht bestreiten.



Im Falle von elektronisch übermittelten Verträgen kann dieses Schutzziel zusammen mit der Authentizität von einiger Wichtigkeit sein. Sehr häufig wird sie allerdings ähnlich wie die Authentizität in Klassifizierungsrichtlinien nicht eingesetzt.

10.6.2 Schutzstufen

Der Schutzbedarf eines Unternehmenswerts wird durch die Zuordnung zu einer Schutzstufe festgelegt. Da nicht jeder Wert gleich wichtig ist, kann auch folgerichtig nicht jeder Wert den gleichen Schutzbedarf haben. Um Prioritäten bei der Festsetzung von Maßnahmen setzen zu können, ist es erforderlich, sich Gedanken zu machen, in welche Schutzstufe ein betrachteter Wert eingeordnet werden muss. Schutzstufen werden zudem üblicherweise in Dokumenten sichtbar gemacht und in den zugehörigen Dateien maschinenlesbar abgelegt. Auf diese Weise kommen Bezeichnungen wie »streng vertraulich« in den Fußzeilen von Präsentationen zustande. In der Klassifizierungsrichtlinie werden die Schutzziele und die Schutzstufen in einen Zusammenhang gebracht und dargestellt. Diese Richtlinie dient dann als Basisdokument, wenn es um die Klassifizierung von Werten geht. Im Kapitel »Organisation von Richtlinien« wird detailliert auf diese Richtlinie eingegangen.

Vor der Erstellung der Klassifizierungsrichtlinie müssen einige Rahmenbedingungen festgelegt werden. Dazu gehören vor allem die Definition der Anzahl von Schutzstufen und wie sich die Abgrenzung zwischen ihnen gestalten soll. In der Praxis wird schnell deutlich, dass in diesem Fall die verschiedensten Einflussfaktoren eine Rolle spielen. Der Wunsch möglichst exakter Bewertungen und dementsprechend viele Stufen stehen dem Wunsch nach einem einfachen System mit wenigen Einstufungen gegenüber.

Wichtig

Wurden in anderen Bereichen wie dem Unternehmensrisikomanagement oder im Entwicklungsprozess (z.B. das Reifegradmodell) bereits Methoden eingeführt, die ein vierstufiges Modell bevorzugen, so kann es hilfreich sein, wenn die Art und Weise der Klassifizierung von Werten zumindest in diesem Punkt ähnlich ist.



Die Klassifizierung von Unternehmenswerten ist eine Aufgabe, die im Grunde jeder Mitarbeiter durchführen kann und muss, und dementsprechend sollten die Methodik und die Klassifizierungsmatrix gestaltet werden. Ziel ist es, dass zwei verschiedene Mitarbeiter bei der Einstufung eines Werts möglichst immer auf dieselbe Schutzstufe kommen.

Als Grundlage für die meisten dieser Einstufungen dienen monetäre Entschuldigungen. Das heißt, dass jeder Stufe Kosten zugrunde liegen, die anfallen, falls das zugehörige Schutzziel nicht erreicht wird. So kann Stufe 2 hinsichtlich der Verfügbarkeit so ausformuliert sein: »Steht das System nicht zur Verfügung, so fallen Kosten im Bereich zwischen 10.000 € und 25.000 € an.«

Weiche Schäden wie z.B. einen Imageverlust einzugruppieren, kann allerdings auch durch noch so exakte Definitionen schwer sein. Es empfiehlt sich, für solche Werte einen unternehmensweit gültigen Katalog anzulegen und die Eingruppierungen darin verbindlich festzulegen.

10.6.3 Prinzipien

Für die Festlegung des Schutzbedarfs haben sich weithin anerkannte Prinzipien durchgesetzt. Im Grunde bilden diese Regeln die Grundpfeiler für die praktische Durchführung einer Risikobewertung. Abhängig von den unternehmerischen Rahmenbedingungen können die Regeln angepasst oder durch zusätzliche Regeln erweitert werden:

- Der Ausfall eines IT-Systems, eines Prozesses oder eines einzelnen Arbeitsplatzrechners kann unter Umständen dazu führen, dass ein Schutzziel wie die Verfügbarkeit an mehreren Stellen verletzt wird. In diesem Fall gilt das **Maximumprinzip**, das besagt, dass der erwartete Schaden im Risikoertrittsfall mit den größten Auswirkungen den Schutzbedarf aller beteiligten Systeme bestimmt.
- Das **Kumulationsprinzip** liegt in den Fällen vor, in denen auf einem Hostsystem z.B. mehrere Programme mit gleichem oder unterschiedlichem Schutzbedarf betrieben werden. In diesem Fall kann zusammen gesehen ein höherer Gesamtschutzbedarf angenommen werden, als es der höchste einzelne Schutzbedarf verlangen würde.
- Technische oder organisatorische Redundanzen wie z.B. ein redundantes IT-System können dazu führen, dass der Schutzbedarf sinkt, da ein paral-



lel arbeitendes System zur Verfügung steht, das im Notfall den Betrieb komplett übernehmen könnte. Diese Konstellation wird im Allgemeinen **Redundanzeffekt** oder **Verteilungseffekt** genannt.

Die Betrachtung von einzelnen Unternehmenswerten kann dazu führen, dass der Blick für das Ganze verloren geht. Es ist wichtig, sich immer wieder von einer übergeordneten Ebene zu nähern. Ein Fall, bei dem der gleichzeitige Ausfall von zwei unwichtig erscheinenden Systemen dazu führt, dass ein als kritisch eingestufter Prozess zum Erliegen kommt, wäre ein solches Beispiel.

10.6.4 Feststellung des Schutzbedarfs

Die Bewertung des Schutzbedarfs eines Wertes stützt sich zumeist auf Vergleiche mit ähnlich gelagerten Vorkommnissen in der Vergangenheit oder wird im Rahmen einer Diskussion unter Experten festgelegt.

Wichtig

Die subjektiv geprägte Betrachtung von Sachverhalten übt einen starken Einfluss auf die Quantifizierung aus. Häufig ist zu erleben, dass durch eine Erhöhung des eigenen Bereichs durch das Mittel der höheren Klassifizierung der eigenen Prozesse Verzerrungen entstehen. Aus diesem Grund ist das Hinterfragen der Werte durch eine möglichst objektive Stelle ein wichtiger Punkt.

Der erste Schritt auf dem Weg, den Schutzbedarf eines Wertes zu ermitteln, ihn also zu klassifizieren, ist der, eine Klassifizierungsrichtlinie zu erstellen. Wie das funktioniert und wie eine solche aussehen kann, können Sie in Abschnitt 4.7.2 nachlesen, der sich mit der Richtlinienstruktur im Unternehmen auseinandersetzt.

Angenommen, die Klassifizierungsrichtlinie liegt vor, dann wird sie eine Klassifizierungsmatrix enthalten, die ähnlich gestaltet sein kann wie in Abbildung 10.9.



		Vertraulichkeit	Verfügbarkeit	Integrität
Stufe 0	Niedriger Schaden (1.000€ - < 5.000€)	Adressaten sind alle Mitarbeiter.	Kritische Prozesse sind nicht beeinträchtigt.	Daten können mit geringem Aufwand berichtigt werden.
Stufe 1	Mittlerer Schaden (5.000€ - < 25.000€)	Adressaten sind ein eingeschränkter Personenkreis.	Arbeitsvorgänge sind gestört. Kernprozesse sind teilweise nicht verfügbar.	Der Aufwand Daten zu berichtigen kann erhöht sein.
Stufe 2	Hoher Schaden (25.000€ - <100.000€)	Adressaten sind einzelne benannte Personen.	Prozesse sind nicht verfügbar. Arbeitsvorgänge sind gestört. Kritische Prozesse sind nur sehr eingeschränkt verfügbar.	Daten sind unbrauchbar und können nicht oder nur lückenhaft korrigiert werden.
Stufe 3	Sehr hoher Schaden (<100.000€)	Adressaten sind durch die Unternehmensleitung benannte Geheimsträger.	Kritische Prozesse können nicht ausgeführt werden.	Kritische Daten sind unbrauchbar und können nicht korrigiert werden.

Abbildung 10.9: Beispielhafte Klassifizierungsmatrix

10

Der verursachte Schaden, wenn ein Risiko eintritt, wird in diesem Beispiel mit einer Stufe von 0 bis 3 bewertet. Jede Stufe und jede Klassifizierung ist an einen potenziellen monetären Schaden gebunden. Die Auswirkungen auf Unternehmensprozesse werden in den Beschreibungsfeldern jeweils erläutert. Auf diese Vereinfachung in Form von groben Skalen greift man dann zurück, wenn Schäden üblicherweise nicht genau beziffert werden können.

Die Einteilung in Stufen, die jeweils Bandbreiten entsprechen, hat Vor- und Nachteile. Während die Vorteile der Darstellung von Bandbreiten darin liegen, dass die Zuordnung im Rahmen einer Befragung leichter fällt, wird es spätestens bei der mathematischen Berechnung schwerer fallen, anzusetzende Zahlen zu definieren. Es wird im Vorfeld zu definieren sein, ob ein »Mittlerer Schaden« mit 5.000 € oder 24.999 € anzusetzen ist. Vermutlich wird es ein Wert in der Mitte sein.

Je größer die Bandbreite, desto weniger genau wird eine Risikoeinschätzung und damit auch der spätere Vergleich von Risiken sein. Je kleiner aber die Bandbreite ist, desto mehr Stufen wird man benötigen. Man kann schnell ersehen, dass der grundlegenden Definition von Stufen und ihren Bandbreiten eine wichtige Rolle zufällt – mit Auswirkungen auf den gesamten IT-Risi-



komanagementprozess. Viele Unternehmen ergänzen ihre Richtlinie zum IT-Risikomanagement um einen Anhang, der diese Festlegungen genau aufzeigt, inklusive einer verbindlichen Festlegung, in welchen Fällen welcher Ansatz zu nutzen ist.

In den meisten Fällen sind Daten der bestimmende Wert, den es maßgeblich zu schützen gilt. Es sind aber durchaus auch andere Konstellationen denkbar. So ist ein handgefertigter Prototyp eines neuen Produkts ein physischer Wert, der geschützt werden muss. Wissen über die Form und eventuell den Herstellungsprozess sind damit im Prototyp selbst wie auch in den Köpfen der Mitarbeiter vorhanden, die die Form hergestellt haben. In Zeiten enger Budgets kann von einem solchen Wert bis zur Vorstellung beim Kunden oder bis zur Einreichung des Patentantrages die Zukunft eines Unternehmens abhängen. Auch wenn keine Maßnahmen für IT-Systeme letztendlich zur Anwendung kommen werden, so kann in diesem Fall trotzdem ein komplettes Risikomanagement durchgeführt werden – inklusive der zutreffenden Maßnahmen.

Bestimmung des Schutzbedarfs im Beispiel

Angenommen, es wird bezogen auf den Einkaufsprozess ein IT-Risikomanagement durchgeführt und demzufolge Daten erhoben. Zu den als Erstes erfassten Informationen gehören die Lieferantendaten. Diese liegen auf dem PC des Einkäufers vor und werden durch eine Applikation namens »Lieferantenverwaltung« verarbeitet. Die Klassifizierung auf Basis der Klassifizierungsrichtlinie umfasst alle drei Schutzziele. Um die Einordnung realitätsnah durchführen zu können, wird der Einkaufsleiter in seiner Funktion als Eigentümer der Daten gebeten, die Klassifizierung durchzuführen.

Der Prozess der Festlegung der Schutzstufen vollzieht sich wie in Abbildung 10.10 gezeigt. Zunächst werden alle Datenarten bestimmt, die für den zu klassifizierenden Prozess von Bedeutung sind. In einem Gespräch wird dann der Dateneigentümer genau festlegen, wie jede Datenart einzustufen ist. Diese Einstufung findet für jedes Schutzziel statt. Aus dieser Festlegung heraus entsteht die grundlegende Liste, auf die im Folgenden aufgebaut wird.



SCHUTZBEDARFSFESTSTELLUNG

Risikoblatt	05082011.73
Verantwortlich	Herr Maier
Asset	DATA01
Risiko 1	Betriebssystem
Risiko 2	Schadsoftware

	Vertraulichkeit	Verfügbarkeit	Integrität
Stufe 0 Niedriger Schaden (1.000€ - < 5.000€)	Adressaten sind alle Mitarbeiter.	Kritische Prozesse sind nicht beeinträchtigt.	Daten können mit geringem Aufwand berichtet werden.
Stufe 1 Mittlerer Schaden (5.000€ - < 25.000€)	Adressaten sind ein eingeschränkter Personenkreis.	Arbeitsvorgänge sind gestört. Kernprozesse sind teilweise nicht verfügbar.	Der Aufwand Daten zu berichtigen kann erhöht sein.
Stufe 2 Hoher Schaden (25.000€ - <100.000€)	Adressaten sind einzelne benannte Personen.	Prozesse sind nicht verfügbar. Arbeitsvorgänge sind gestört. Kritische Prozesse sind nur sehr eingeschränkt verfügbar.	Daten sind unbrauchbar und können nicht oder nur lückenhaft korrigiert werden.
Stufe 3 Sehr hoher Schaden (<100.000€)	Adressaten sind durch die Unternehmensleitung benannte Geheimnisträger.	Kritische Prozesse können nicht ausgeführt werden.	Kritische Daten sind unbrauchbar und können nicht korrigiert werden.



Lfd. Nr.	Unternehmenswert (Asset)	Schutzbedarfsfeststellung			
		Vertraulichkeit	Verfügbarkeit	Integrität	Beschreibung
A1	DATA01	Stufe 1 (mittel)	Stufe 2 (hoch)	Stufe 1 (mittel)	Datenserver enthält Produktionsdaten und muss stets verfügbar sein.
A2					

Abbildung 10.10: Klassifizierung eines Unternehmenswerts

Prozess	Einkaufsprozess
Bestimmender Wert	Lieferantendaten
Beteiligte Werte	PC des Einkäufers, Applikation Lieferantenverwaltung, Server
Vertraulichkeit	2 (mittel)
Verfügbarkeit	2 (hoch)
Integrität	3 (sehr hoch)

Abbildung 10.11: Schutzbedarfsfeststellung am Beispiel

Der Einkaufsleiter argumentiert, dass diese Daten wichtig für das Unternehmen sind, aber ein Verlust keine existenziellen Probleme aufwerfen würde.



KAPITEL 10 – IT-RISIKOMANAGEMENT

An der Verfügbarkeit hängen zwar die Einkäufer, diese könnten sich aber für einen gewissen Zeitraum auch anderen Aufgaben widmen, falls der Zugriff auf diese Daten unterbrochen würde. Bezuglich der Integrität wählt er die höchste Schutzklasse, da diese Daten ständig angepasst werden und selbst die Backups nur unvollständig vorliegen. Aus diesem Grund wäre eine Verfälschung der Daten schwer zu bemerken und danach nicht vollständig wieder umzukehren.

10

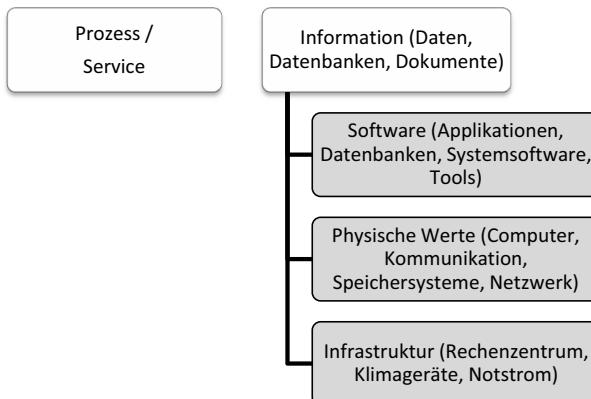


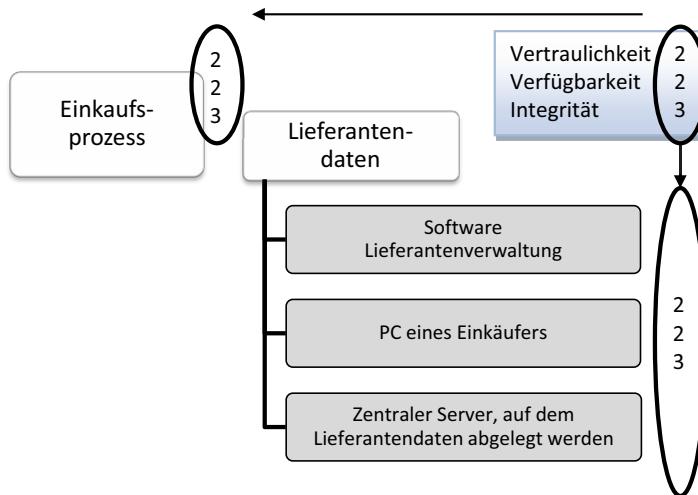
Abbildung 10.12: IT-Systeme, die den Einkaufsprozess unterstützen

Angenommen, es werden vorrangig die Lieferantendaten als entscheidend für den Prozess »Einkaufsprozess« definiert, so leitet sich aus deren Klassifizierung auch die Einstufung des **Gesamtprozesses und der unterstützenden IT-Systeme ab**. Eine Aufstellung dieser grundlegenden Systeme ist in Abbildung 10.13 zu sehen. Es handelt sich dabei sowohl um Applikationen als auch um physische Server und die Räumlichkeiten, in denen diese untergebracht sind. Für alle diese weiteren Werte müssen nun die gleichen Anforderungen angesetzt werden, wie sie für den Gesamtprozess bzw. die zugrunde liegenden Daten definiert wurden. Daraus können die zu tätigenden Anstrengungen abgeleitet werden, die nun eingeleitet werden müssen, um auch diese Systeme angemessen sicher zu gestalten und zu betreiben.

In Abbildung 10.13 wird der Zusammenhang noch deutlicher. In dieser Abbildung werden bereits die expliziten Gerätschaften und Softwareprodukte aufgeführt, die im Geltungsbereich der Betrachtung liegen. Aus dieser Auflistung kann nun jederzeit abgelesen werden, welche Systeme im Rahmen der Risikoanalyse bearbeitet werden müssen und wie ihre Priorität einzuschätzen ist.



SCHUTZBEDARFSFESTSTELLUNG



10

Abbildung 10.13: Vererbung von Schutzstufen

10.6.5 Veränderung des Schutzbedarfs

Der einmal definierte Schutzbedarf eines Wertes ist Veränderungen unterworfen. Auslöser für diese Änderungen können die unterschiedlichsten Faktoren sein. Der wichtigste Faktor ist die Zeit. Eine Konstruktionszeichnung wird, beginnend in der Vorentwicklung bis hin zur Serienproduktion des Produkts, vermutlich an Wichtigkeit verlieren. Das bezieht sich vor allem auf das Schutzziel Vertraulichkeit. Die Integrität der Daten, die während des Produktionsprozesses genutzt werden, kann im Gegenzug sogar an Wichtigkeit gewinnen, da die Kosten im Falle des Verlustes der Integrität höher sein könnten als zu Beginn der Entwicklung. Die Darstellung dieser Faktoren ist sehr komplex und fehleranfällig. Die einzelnen Phasen sind in Abbildung 10.14 dargestellt.

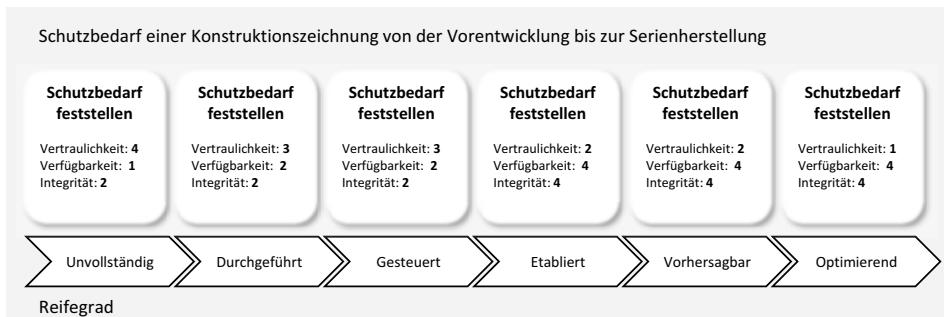


Abbildung 10.14: Veränderung des Schutzbedarfs



Es ist zu empfehlen, den Lebenszyklus eines kritischen Unternehmenswerts z.B. anhand des Reifegradmodells (SPICE) darzustellen und für jeden Abschnitt eine Einstufung vorzunehmen.

Neben der reinen Zeit spielen Parameter wie neue angrenzende Systeme, neue Versionen von Software, Backup-Systeme, Einführung von redundanten, ausfallsicheren Systemen, also im Großen und Ganzen alle Veränderungen, die den betrachteten Wert berühren, eine Rolle. Hilfreich sind deshalb Übersichten über Zusammenhänge und Prozessabläufe, um diese Veränderungen auch visuell nachvollziehbar zu machen.

10.6.6 Widersprüchliche Schutzziele

10

Klassifiziert werden können alle Wertearten. Meistens wird es sich aber um Daten handeln, also Informationen in elektronisch abgelegter Form. Dabei können divergierende Schutzziele auftauchen. Für die Datenart »Finanzdaten« beeinflussen sich z.B. die Schutzziele »Verfügbarkeit« und »Vertraulichkeit« häufig gegenseitig. Will man die Vertraulichkeit z.B. durch eine Verschlüsselung der Daten erhöhen, so kann sich das negativ auf die Verfügbarkeit auswirken, da je nach Infrastruktur nicht mehr von jedem System auf diese Daten zugegriffen werden kann. Wenn man andersherum die Verfügbarkeit z.B. eines E-Mail-Systems erhöhen will, so muss man unter Umständen die Freigabe für weniger gut gesicherte Lesegeräte wie Smartphones erteilen, obwohl darunter das Schutzziel Vertraulichkeit leiden könnte. Weitere Antagonisten sind z.B. die Umsetzung von Authentizität und das Recht auf Pseudonymisierung oder gar Anonymisierung von Daten aufgrund des Datenschutzrechts.

Diese unterschiedlichen Sichtweisen können bedingen, dass bei der Klassifizierung von Werten jedes Schutzziel gesondert betrachtet und der Einfluss auf andere Schutzziele ausgeblendet wird. In jedem Fall ist es sinnvoll, die Vorgehensweise in diesen Fällen vorab festzulegen und in der Klassifizierungsrichtlinie festzuhalten.

10.6.7 Schadensklassen

Die Schäden, die beim Nichterreichen eines oder mehrerer der betrachteten Schutzziele entstehen könnten, lassen sich typischerweise bestimmten Schadensklassen zuordnen. Häufig treffen dabei für einen Schaden mehrere Schadensklassen zu. So kann der Ausfall eines Webservers sowohl die Aufga-



benerfüllung innerhalb eines Geschäftsprozesses beeinträchtigen als auch direkte finanzielle Einbußen nach sich ziehen und einen Imageverlust zur Folge haben. Zusätzliche Schadensklassen sollten immer vorab abgestimmt werden.

Übliche Schadensklassen sind:

- Imageschäden
- Finanzielle Schäden
- Gesetzesverstoß
- Persönliche Unversehrtheit
- Beeinträchtigung der Aufgabenerfüllung
- Beeinträchtigung des informationellen Selbstbestimmungsrechts

10

10.6.8 Abbildung des Datenflusses

Die Verarbeitung und der Austausch von Daten innerhalb von IT-Systemen und zwischen IT-Systemen kennzeichnen die moderne Informationstechnologie. Jedes System, das in einem solchen Datenaustauschverbund angesiedelt ist, kann man sich als Knotenpunkt vorstellen. Angewandt auf die Systematik des IT-Security-Managements bedeutet dies, dass die im Verbund mehrerer Knoten zirkulierenden Daten mit einer Klassifizierung versehen werden sollen. Dasselbe gilt für die Knotenpunkte bzw. IT-Systeme, die diese Daten bearbeiten und verarbeiten. Ziel ist, dass Daten ihrer Schutzklasse entsprechend nur zu Knotenpunkten fließen dürfen, deren Klassifizierung gleich oder höher ist als die der Daten. Ein Beispiel für einen Datenfluss ist die Übermittlung von Daten in einem Netzwerk. Die Knoten repräsentieren dabei aktive Netzwerkkomponenten.

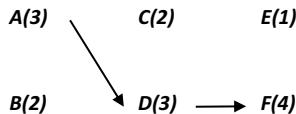


Abbildung 10.15: Datenfluss und Klassifizierung

In Abbildung 10.15 werden die IT-Systeme A, B, C, D, E und F dargestellt. Die für sie jeweils definierte Klassifizierung, in diesem Fall bezüglich des Schutz-



ziels Verfügbarkeit, wird in Klammern angezeigt. So ist IT-System A in die Klassifizierungsstufe 3 eingeordnet. Sollen nun Daten der Klassifizierung 3 verarbeitet werden, so ist dies über diejenigen IT-Systeme möglich, die der Stufe 3 oder höher zugeordnet sind. Wird festgestellt, dass ein IT-System diesem Kriterium nicht entspricht, so muss mittels einer Risikobehandlungsstrategie festgelegt werden, wie mit diesem Risiko umzugehen ist. Üblicherweise wird durch Ergreifung von Maßnahmen dafür Sorge getragen, dass auch dieses IT-System insoweit abgesichert wird, dass es auch mindestens der Klassifizierungsstufe 3 entspricht.

Aufwendig ist, dass in diesem Beispiel jede Beziehung zwischen Knotenpunkten überprüft werden muss. So wird für A, C, D und F jeweils geprüft, ob die Klassifizierung des Knotens höher oder gleich der Klassifizierung der Daten ist. Summa summarum ergeben sich damit vier Einzelprüfungen.

10



Abbildung 10.16: Ebenendarstellung von Knoten und ihrer Klassifizierung

Wenn man die Darstellung etwas verändert, so kann man aus der Transitivität der Knotenbeziehungen Kapital schlagen. In Abbildung 10.16 sind die höher angeordneten Knotenpunkte jeweils diejenigen, die einer höheren Schutzklasse genügen. Auf gleicher Ebene angeordnete Knoten entsprechen der gleichen Schutzklasse. Sollen Daten der Klassifizierungsstufe 3 verarbeitet werden, so kann dies zwischen allen Knoten der oberen Ebene erfolgen.

10.6.9 Entscheidungsfindung auf Basis des Schutzbedarfs

Der Feststellung des Schutzbedarfs folgen das Risikomanagement und letztendlich die Definition von Maßnahmen. Das ist eine übliche Vorgehensweise. Im täglichen Betrieb kann dieser Handlungsstrang umgedreht und im Grunde eine ganze Reihe von täglichen Entscheidungsprozessen daran gekoppelt werden.



Angenommen, es sollen neue Multifunktionsdrucker für einzelne Bereiche des Unternehmens angeschafft werden, dann könnten neben den üblichen technischen Features auch konkrete Sicherheitsanforderungen als Entscheidungsgrundlage herangezogen werden.

Eine Angebotsliste für die verschiedenen Bereiche könnte wie folgt aussehen:

- Drucker 1: Für unbedenkliche Ausdrucke
- Drucker 2: Für vertrauliche Ausdrucke
- Drucker 3: Für geheime Ausdrucke

Die drei genannten Druckertypen entsprechen jeweils einer anderen Klassifizierung und kosten je nach Sicherheitsstufe auch mehr in der Anschaffung. So werden bei Druckertyp 3 nach jedem Druck alle Druckdaten auf der internen Festplatte dreimal überschrieben. Bei Druckertyp 1 ist dies grundsätzlich nicht der Fall.

Im nächsten Schritt werden die Druckertypen den Abteilungen angeboten. Das Gespräch zwischen einem Abteilungsleiter und dem zuständigen IT-Mitarbeiter könnte dann wie folgt aussehen:

Abteilungsleiter: »Wir benötigen einen Drucker, am besten den größten, sichersten und günstigsten.«

IT-Mitarbeiter: »Welcher Klassifizierung entsprechen die sensiblen Daten, die in Ihrer Abteilung ausgedruckt werden?«

Abteilungsleiter: »Laut Richtlinie Stufe 2 von insgesamt 3.«

IT-Mitarbeiter: »Gut, dann ist Druckertyp 2 für Sie passend.«

Die Entscheidung, die auf der Klassifizierung der zu druckenden Daten basiert, ist formal nachvollziehbar und leicht zu dokumentieren. Darin liegt der große Vorteil bei dieser Art von Vorgehensweise.

Neben Drucken wird z.B. auch die Auswahl von Speicherorten von Dateien nach diesem Prinzip vorgenommen. In diesem Fall hält die IT-Abteilung mehrere Server bereit, die verschiedenen Stufen in der Klassifizierung entsprechen. Dazu gehören Server in speziell gesicherten Umgebungen, Server im Rechenzentrum oder Server, die nicht besonders geschützt werden. Abhängig von den Daten erfolgt die Auswahl des Servers, was wiederum auch unterschiedliche Kosten zur Folge hat.



10.7 IT-Risikomanagement Prozess

Bislang wurden vor allem die Grundlagen beschrieben, die als Rahmengerüst für die Durchführung eines IT-Risikomanagements erforderlich sind. In den folgenden Unterkapiteln soll der Prozess des IT-Risikomanagements Schritt für Schritt dargestellt werden.

10.7.1 Risiken identifizieren

Der erste Schritt auf dem Weg zur Ermittlung und späteren Bewertung von Risiken ist die Festlegung, welche Unternehmenswerte auf welche Risiken untersucht werden sollen. Es ist leicht einsehbar, dass dies nicht für jede Datenart, für jedes IT-System und auch nicht hinsichtlich eines jeden möglichen Risikos möglich ist. An dieser Stelle helfen die Ergebnisse der Klassifizierung von Prozessen und der Business-Impact-Analyse weiter, die für das Unternehmen wichtigsten Unternehmenswerte zu identifizieren. Dieser Ansatz ist im Endeffekt sehr effektiv, da man sich hier auf die wesentlichen Werte konzentrieren und einen risikofokussierten Ansatz verfolgen kann. Sind solche Listen nicht verfügbar und die Anzahl der vorhandenen Werte überschaubar, dann können die Systeme auch der Reihe nach einzeln betrachtet und einem Risikomanagement unterzogen werden.

Bevor man sich bei der Aufnahme der Risiken übernimmt, macht es Sinn, eine Eingrenzung des Untersuchungsbereichs vorzunehmen. Dieser Untersuchungsbereich wird auch »Geltungsbereich« oder »Scope« genannt. Er definiert, welche Werte in der Untersuchung eine Rolle spielen sollen, und dokumentiert parallel, für welche Werte und Risiken dies nicht der Fall ist.

Zu Beginn der Risikoermittlung steht die Zusammenstellung eines geeigneten Teams. Dieses sollte aus Mitarbeitern der IT-Abteilung und aus Mitgliedern der betroffenen Fachbereiche bestehen. Die IT liefert das erforderliche Hintergrundwissen, um Prozessen und Abläufen die unterstützenden IT-Systeme zuzuordnen. Die Fachabteilungen beurteilen den Grad an Vollständigkeit. Zusammen wird der Geltungsbereich bestimmt und dann die darin enthaltenen Unternehmenswerte zusammengestellt und dokumentiert.

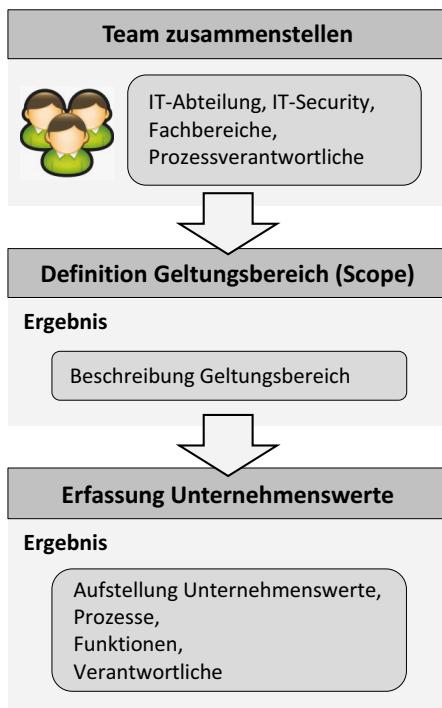


Abbildung 10.17: Identifizierung der zu untersuchenden Unternehmenswerte

Hinweis

Die Hauptaufgabe des Managers IT-Security liegt in der Moderation und Steuerung des Teams. Er bringt das erforderliche Grundwissen über den Vorgang des IT-Risikomanagements mit und kann Risiken oft schneller und umfassender erkennen und beurteilen, als es den Personen aus dem Fachbereich möglich wäre. Als Schnittstellenfunktion zwischen den Mitarbeitern aus der IT und den Dateneigentümern hat er zudem die spannende Aufgabe, zwischen den jeweiligen Standpunkten zu vermitteln.

Geltungsbereich festlegen

Der Geltungsbereich beschreibt den Ausschnitt innerhalb des Unternehmens, der von der aktuellen Risikoermittlung betrachtet werden soll. Unternehmenswerte innerhalb des Geltungsbereichs werden untersucht, Unter-



nehmenswerte außerhalb des Geltungsbereichs werden nicht erfasst. Diese Abgrenzung ist erforderlich, um speziell in größeren Unternehmen den Aufwand für diesen Prozessschritt abschätzen und auch bewältigen zu können.

Die Herausforderung liegt darin, dass faktisch jedes System mit vielen anderen Systemen vernetzt ist: zum einen über die Netzwerkinfrastruktur, zum anderen durch Mechanismen wie z.B. den schlichten Datenaustausch. Betrachtet man nun Systeme singulär und lässt angeschlossene Systeme außen vor, so ist eine geeignete Aussage über das Risiko schwer oder schlicht nicht sinnvoll möglich.

Betrachtet man einen Webserver und definiert Clients, die darauf zugreifen, sowie den angeschlossenen Datenbankserver als außerhalb des Geltungsbereichs stehend, dann wird die Liste an Bedrohungen und Schwachstellen lückenhaft bleiben. In diesem Fall wäre es besser, man würde den Webserver, den Datenbankserver und exemplarisch einige Clientinstallationen als Gesamtsystem betrachten und untersuchen.

10

Angenommen, es handelt sich bei der aktuellen Risikoermittlung nicht von vornherein um eine definierte Aufgabenstellung wie zum Beispiel: »Untersuchen Sie doch bitte mal das E-Mail-System auf Risiken und ermitteln Sie erforderliche Maßnahmen.« Falls es sich also um eine Aufgabe handelt, die eher den Vorgaben »Untersuchen Sie bitte das Rechenzentrum und alle dortigen IT-Systeme auf Risiken« entspricht, dann ist es von einem Belang, von vornherein auf die korrekte Festlegung des Geltungsbereichs zu dringen. In diesem zweiten Fall ist noch wichtiger, in die technische Betrachtung auch die organisatorische und strategische Ausrichtung des Unternehmens mit einzubeziehen. So sollten folgende, zusätzliche Aspekte Einfluss auf die Ausgestaltung des Geltungsbereichs nehmen:

- **Die Unternehmensstrategie und davon abgeleitet die IT-Strategie sowie der Geschäftszweck:** Sind ein Prozess oder definierte Daten und daraus abgeleitet bestimmte IT-Systeme für die Unternehmensstrategie von herausragender Bedeutung, so wäre es nicht im Sinne des Unternehmens und einer ganzheitlichen Risikostrategie, wenn diese Systeme bei der Risikobetrachtung außen vor blieben.
- **Geschäftsprozesse:** IT-Systeme unterstützen Arbeitsabläufe und Geschäftsprozesse. Der Geltungsbereich sollte so gewählt werden, dass Prozesse in ihrer Gänze abgedeckt werden. So wäre es nicht ausreichend, wenn IT-Sys-



teme des Prozesses »Versand«, z.B. Drucker für Verladescheine, nicht berücksichtigt werden, alle anderen IT-Systeme, die diesen Prozess unterstützen, aber schon.

- **IT-Compliance, Vorgaben von Kunden und Lieferanten sowie interne Richtlinien:** Definierte Vorgaben, die aus dem Unternehmen oder von außen kommen, müssen mit in die Ausgestaltung des Geltungsbereichs eingebbracht werden.
- **Unternehmensrisikomanagement:** Ist das IT-Risikomanagement in das Unternehmensrisikomanagement eingebettet oder werden Methoden übergreifend genutzt, so stellen diese Rahmenbedingungen dar, die einzuhalten sind.
- **Lokale Gegebenheiten:** Kulturelle und länderspezifische Eigenheiten sollten in die Überlegungen mit eingebunden werden.

Eine stringente Betrachtungsweise erfordert, dass explizite Ausnahmen, d.h. Werte, die aus dem Geltungsbereich entfernt werden, obwohl sie aufgrund einer oder mehrerer Rahmenbedingungen Bestandteil sein sollten, auch als solche Ausnahmen (*exceptions*) benannt und dokumentiert werden.

Die Feststellung des Geltungsbereichs erfolgt immer für die jeweils geplante Risikoanalyse. Im Rahmen einer Vorbereitung für eine Zertifizierung größeren Umfangs oder falls es sich um ein sehr komplexes Untersuchungsobjekt handelt wie z.B. ein Produktionssystem, wird der Geltungsbereich dementsprechend sehr viel umfangreicher gewählt, und die Teams werden dementsprechend anders zusammengesetzt sein.

Es ist wichtig, zu verstehen, dass der gesamte Vorgang der Definition eines Geltungsbereichs, die Ermittlung darin befindlicher kritischer Systeme und danach die Identifizierung von Risiken komplex und fehlerträchtig ist. Auch hier empfiehlt sich, eine möglichst formale und nachvollziehbare Vorgehensweise zu wählen.

Unternehmenswerte erfassen und katalogisieren

Im Grunde ist die Aufstellung der zu untersuchenden Unternehmenswerte ein Ausschnitt aus einem Assetmanagement und listet alle Werte auf, für die ein IT-Risikomanagement durchgeführt werden soll. Der Strukturierung dieser Liste kommt dabei eine hohe Bedeutung zu, insbesondere dann, wenn es sich um viele und komplex miteinander vernetzte Systeme handelt.



KAPITEL 10 – IT-RISIKOMANAGEMENT

Vorarbeit, die in diesem Stadium geleistet wird, kann die weitere Vorgehensweise stark erleichtern. Die Gruppierung der Werte kann unter geografischen oder organisatorischen Gesichtspunkten katalogisiert werden. Eine Mischung beider Varianten ist empfehlenswert.

10

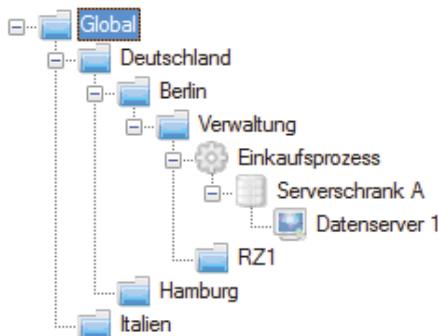


Abbildung 10.18: Verwaltung von Werten innerhalb einer Prozessstruktur

In Abbildung 10.18 erfolgt die Einordnung von Werten, in diesem Fall der »Datenserver 1«, in Bezug auf einen Prozess. Der Prozess selbst wird geografisch der Region Berlin und dem Land Deutschland zugeordnet. Diese Zuordnung erlaubt es, mehrere Informationen gleichzeitig abzulegen, und erleichtert die spätere Diskussion, da viele erforderliche Parameter bereits visualisiert vorliegen.

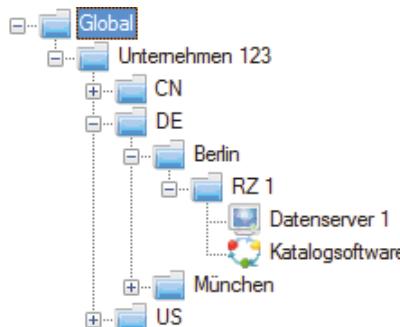


Abbildung 10.19: Verwaltung von Werten in einer geografisch geordneten Struktur

In Abbildung 10.19 werden Unternehmenswerte ausschließlich geografisch geordnet angegeben. Die verschiedenen Arten von Werten wie Computer, Software, Daten, Dienstleistungen usw. sind weitere wichtige Ordnungskri-



terien, die in diesem Fall durch unterschiedliche Typen dargestellt werden können.

10.7.2 Risikoermittlung

In der Praxis wird die Anzahl der Unternehmenswerte deutlich höher sein als die Anzahl möglicher Risiken. Aus diesem Grund empfiehlt die ISO 27001 in der Fassung von 2013, vonseiten der Risiken und nicht der Unternehmenswerte an die Risikoermittlung heranzugehen. Ein gangbarer Kompromiss ist es, Listen der besonders kritischen Werte in den Mittelpunkt zu setzen und darauf eine Risikoermittlung aufzubauen. Dieser Top-down-Ansatz erlaubt es schnell, die wichtigsten Systeme sicher zu betreiben. Erst die unternehmensexternen Software-Plattformen, dann die dazu erforderlichen Server und Datenbanken, dann die Rechenzentren, in denen diese Systeme untergebracht sind, und die Netzwerkinfrastrukturen, die man zur Kommunikation benötigt. Dieser Ansatz definiert Prioritäten und verliert sich nicht in der Erfassung des letzten Arbeitsplatzrechners.

In einem weiteren Schritt, der natürlich auch parallel angegangen werden kann, empfiehlt es sich, die wichtigsten Risiken zu definieren und von ihnen ausgehend die betroffenen Werte zu identifizieren und einem Risikomanagement zu unterwerfen. Ein typisches Beispiel dafür ist die Schadsoftware WannaCry. WannaCry verkörpert die Bedrohung, dass ein befallenes IT-System verschlüsselt und dadurch im schlimmsten Fall unbrauchbar wird. Stellt man dieses Risiko in den Vordergrund, dann ist der logische, nächste Schritt der, alle Arbeitsplatzrechner und Server zu identifizieren, die von dieser Schadsoftware befallen werden könnten, und diese entsprechenden Maßnahmen zu unterwerfen.

In beiden Fällen gibt es eine direkte Verknüpfung von Unternehmenswert und Risiko und dadurch wird es deutlich leichter, Statistiken abzuleiten und den aktuellen Stand der Sicherheit in einer Risikoübersicht abzubilden.

Bedrohungslisten

Bedrohungslisten dienen der Standardisierung der Risikoermittlung. Im Grunde handelt es sich dabei um eine Auflistung möglicher Bedrohungsszenarien, die so weit vorbereitet wurde, dass passende Bedrohungen direkt den betroffenen Wertekategorien zugeordnet werden können. Durch sie soll



KAPITEL 10 – IT-RISIKOMANAGEMENT

gewährleistet werden, dass alle Stellen, die eine Bedrohungsanalyse vornehmen, immer die gleiche Nomenklatur benutzen. Sind bereits Bedrohungslisten im Unternehmen vorhanden, so sollten diese herangezogen werden, um mögliche Risiken je Unternehmenswertetyp (*asset type*) abzuleiten und zu dokumentieren.

In Abbildung 10.20 wird der Unternehmenswert »DATA01« der Werteart »Server« zugeordnet. Aus der Bedrohungsliste für Server können eine Reihe von Standardbedrohungen abgelesen werden. Das Team entscheidet sich, dass zwei Risiken für den Unternehmenswert zutreffend sind, und notiert dies auf einem Risikoblatt.

10

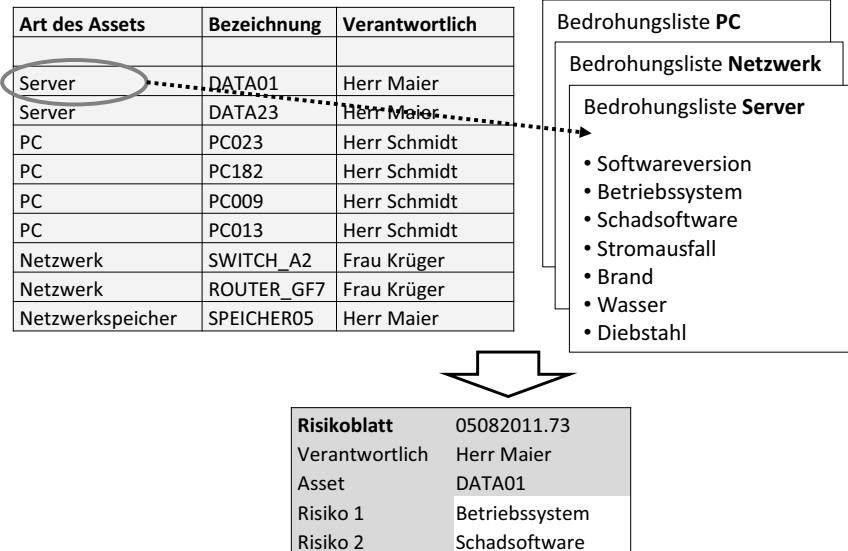


Abbildung 10.20: Zuordnung von Bedrohungen aus vorbereiteten Listen

Es ist wichtig zu bedenken, dass eine Bedrohung nur dann zu einem wirksamen Risiko führen kann, wenn für die Bedrohung auch eine Schwachstelle existiert. Ist z.B. für die Werteklasse »Server« die Bedrohung »Missbräuchliche Nutzung des USB-Ports« festgelegt, so kann diese Bedrohung nur für diejenigen Server zu einem Risiko führen, die auch über die Schwachstelle USB-Port verfügen. In der Praxis kann man davon ausgehen, dass bei Bedrohungen wie »Schadsoftware« oder »Fehler im Betriebssystem«, die eher einen allgemeinen Charakter haben, immer auch eine entsprechende Schwachstelle vorhanden ist.



Individualrisiken

Neben den Standardbedrohungen sind für jeden Unternehmenswert auch individuelle Risiken zu ermitteln, die durch vorgehaltene Bedrohungen auf Standardlisten nicht abgedeckt werden. Eine Möglichkeit, diese Risiken aufzudecken, ist ein Fachgespräch, zu dem Administratoren, Personen aus dem Fachbereich und der IT-Security sowie unter Umständen externe Berater eingeladen werden. Die Art des Gesprächs kann von einem einfachen Brainstorming oder Interview bis hin zu Befragungsverfahren wie z.B. der Delphi-Methode reichen. Der Vorteil der Delphi-Methode ist, dass viel Wert darauf gelegt wird, dass sich Aussagen verschiedener Personen nicht gegenseitig beeinflussen bzw. verstärken.

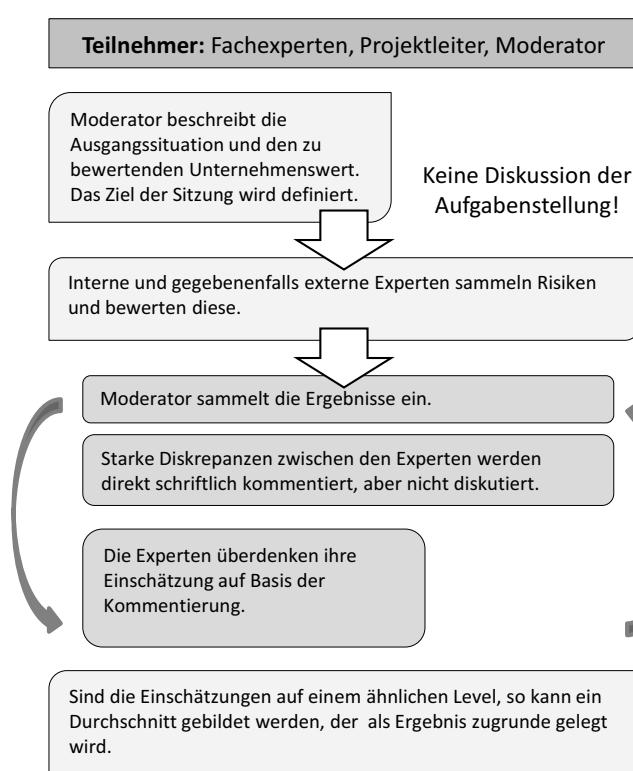


Abbildung 10.21: Standard-Delphi-Methodik

Die Delphi-Methode kann zur Risikoermittlung, aber auch zur Risikobewertung herangezogen werden. Insbesondere die Faktoren Eintrittswahrschein-



lichkeit, potenzieller Schaden und die Schutzbedarfsfeststellung können so auf eine weitgehend objektive Art und Weise definiert werden.

Es ist zu beachten, dass abhängig von der Fragestellung unterschiedliche Personenkreise hinzugezogen werden sollten. So wird die Schutzbedarfsfeststellung mit dem betroffenen Fachbereich durchgeführt werden, während die Erfassung von Risiken als technisches Thema eher zusammen mit der IT-Abteilung stattfinden wird.

10.7.3 Risikobewertung

Die Risikobewertung hat die Aufgabe, die ermittelten Risiken näher zu spezifizieren und quantitativ und qualitativ zu bewerten. Dieser Schritt muss am Ende alle Informationen bereitstellen, die für eine Risikobehandlung benötigt werden. Auf Basis der Ergebnisse aus der Risikobewertung werden dann letztendlich Maßnahmen abgeleitet.

Um diesen Punkt bearbeiten zu können, müssen etliche Rahmenbedingungen mit ins Kalkül gezogen werden. Dazu gehören z.B. alle Maßnahmen, die bereits heute getroffen wurden, um ein Risiko zu vermindern, oder Erkenntnisse darüber, ob das Risiko bereits durch Dritte getragen wird, also eine Art Versicherung abgeschlossen wurde. Ein weiterer Punkt ist das Wissen darüber, ob Folgen eines Risikos im Eintrittsfall überhaupt rechtzeitig erkannt werden würden und ob es einen Business-Continuity-Plan gibt, der für diesen Fall Notfallprozeduren vorsieht.

Ungenauigkeiten begleiten den gesamten Prozess der Risikoanalyse. Ein Großteil der Bewertungen basiert nicht auf fixen Zahlen und absolutem Wissen, sondern auf Erfahrungswerten von darüber befragten Personen. Ergeben sich konkrete Anhaltspunkte für Ursachen, die zu fehlerhaften Festlegungen führen können, so sollten diese diskutiert und dokumentiert werden. Im Rahmen des Lebenszyklus des IT-Security-Managements kann auf diese Aufzeichnungen in der Phase der Überprüfung wieder zurückgegriffen werden. Werden z.B. Risiken für eine Serverhardware gesammelt und ist bekannt, dass sich der Hersteller ändern wird, so kann dies notiert und im Überprüfungslauf in die Überlegungen integriert werden. Unter Umständen führt eine solche Unsicherheit nach der späteren Überprüfung zu einer veränderten Risikoeinschätzung.



Eintrittswahrscheinlichkeit

Einzuschätzen, mit welcher Wahrscheinlichkeit ein Risiko eintreten wird, ist eine Herausforderung, da es quasi unmöglich ist, alle Parameter zu kennen, die Einfluss darauf nehmen können. Das wichtigste Hilfsmittel ist die Statistik. Mit ihrer Hilfe wird durch Auswertung von Ereignissen aus der Vergangenheit die Eintrittswahrscheinlichkeit errechnet, vermindert durch in der Zwischenzeit eingeführte risikoreduzierende Maßnahmen. Wegen dieser Schwierigkeiten ist es wichtig, eine möglichst formale Vorgehensweise vorzugeben, um ermittelte Daten glaubhaft vertreten zu können. Dies gilt vor allem für den Fall, wenn es darum geht, dass kostenintensive Maßnahmen daraus abgeleitet werden.

Grundsätzlich können folgende Vorgehensweisen angewendet werden:

- Erfahrungen aus der Vergangenheit stellen eine der wichtigsten Kennzahlen dar. Wie häufig ist das Ereignis bereits pro Zeitraum aufgetreten? Wie haben sich implementierte Maßnahmen auf die Eintrittswahrscheinlichkeit ausgewirkt? Wenn diese Fragen beantwortet werden können, so ist eine Projektion in die Zukunft aussagekräftig. Statistische Voraussagen werden mit steigender Anzahl von Werten, mit denen operiert wird, präziser werden, und deshalb wird dieses Verfahren vor allem bei häufig auftretenden Ereignissen die beste Vorgehensweise darstellen. Zu diesen Risikoeintritten gehören z.B. Vorfälle wie das Auftreten von Schadsoftware pro Jahr pro Rechner oder insbesondere in Standorten mit schwach ausgebauter öffentlicher Infrastruktur der Ausfall von Strom oder Wasser pro Jahr.
- Vergleiche mit anderen Unternehmen sind ein zweiter Ansatz, der dem ersten nahe kommt. In diesem Fall werden aus vergangenen Ereignissen gefütterte Statistiken von anderen, vergleichbaren Unternehmen zur Analyse herangezogen. Bereinigt um unternehmensspezifische Faktoren stellt dies häufig die einzige Möglichkeit dar, auf verlässliches Zahlenmaterial zugreifen zu können. Vor allem bei Vorfällen mit wenigen Ereignissen pro Jahr stellt dies eine wertvolle Hilfe dar. Alternativ zu diesen Statistiken können auch externe Berater herangezogen werden, die ihren Erfahrungsschatz mit einbringen.
- Wahrscheinlichkeitsvorhersagen auf Basis induktiver Verfahren (*inductive reasoning techniques*) sind eine weitere Möglichkeit, formal an die Probleme



matik heranzugehen. In ISO 31010 wird in diesem Zusammenhang die Fehlzustandsbaumanalyse und Ereignisbaumanalyse genannt. Diese Verfahren basieren auf einer Analyse, die untersucht, wie sich Ereignisse unterschiedlichster Art auf das Gesamtsystem auswirken. In einem Prozess wird jeder Teilschritt betrachtet, der jeweilige Ausfall markiert und die Folgen für die weiteren Schritte untersucht. Dies erfolgt in einer fortlaufenden Fallunterscheidung »Ereignis ist eingetreten« bzw. »Ereignis ist nicht eingetreten«. Beide Möglichkeiten werden bei jedem Schritt weiter untersucht und auf jeder Ebene mit einer Eintrittswahrscheinlichkeit verknüpft. Die Gesamteintrittswahrscheinlichkeit errechnet sich dann aus allen Einzelteintrittswahrscheinlichkeiten.

- Ermittlung der Eintrittswahrscheinlichkeit durch Interviews mit den internen und gegebenenfalls externen Fachleuten in strukturierten Sitzungen. Hier bietet sich wiederum die Standard-Delphi-Methode, siehe Abbildung 10.21, an, um zu einem möglichst objektiven Gesamtbild zu kommen, das letztendlich auch alle Experten gemeinsam tragen können.

10

Die Eintrittswahrscheinlichkeit wird meistens in Stufen angegeben, da es sich um eine geschätzte Vorhersage handelt, die per se ungewiss ist. Diese Stufen können z.B. folgendermaßen ausgestaltet sein:

- Stufe 0: 0–1 Ereignisse/Jahr
- Stufe 1: <5 Ereignisse/Jahr
- Stufe 2: <=10 Ereignisse/Jahr
- Stufe 3: >10 Ereignisse/Jahr

Ein Auftreten von Schadsoftware wird vermutlich im Bereich der Stufe 3 eingeordnet werden, der Ausfall des Core Switches, der den Mittelpunkt des internen Netzwerks darstellt, hoffentlich auf Stufe 0. Im letzteren Fall kann die Existenz eines redundanten, zweiten Core Switches zu dieser positiven Einschätzung führen. Der Eintritt des Risikos hätte in diesem Fall eine sehr viel niedrigere Eintrittswahrscheinlichkeit.

Als Bezugszeitraum wird in diesem Beispiel ein Jahr herangezogen. Genauso üblich ist es die Ereignisse pro Produktentwicklungszyklus, z.B. alle 5 Jahre, oder hochgerechnet auf 100 Jahre anzugeben. Diese Bezugsgröße ist wichtig, wenn es darum geht, vergleichbare Berichte zu erstellen.



Potenzieller Schaden

Neben der Eintrittswahrscheinlichkeit ist die Darstellung der Wichtigkeit eines Unternehmenswerts die zweite wichtige Komponente, um ein Risiko rechnerisch darstellen zu können. Diese Wichtigkeit drückt sich bei der Berechnung eines Risikos im Wert »potenzieller Schaden« aus.

Die Schutzbedarfsfeststellung beschreibt damit den potenziellen Schaden, den der Verlust der Sicherheitsziele in Bezug auf den Unternehmenswert für das Unternehmen hätte. Die Schutzbedarfsfeststellung muss formalen Kriterien folgen, um sicherzustellen, dass ein damit berechnetes Risiko stets vergleichbar mit anderen Risiken anderer Werte bleibt. Die Grundlage bildet die Klassifizierungsrichtlinie, in der die Kriterien für die Schutzbedarfsfeststellung dokumentiert sind.

Die Erfassung des potenziellen Schadens fällt den Verantwortlichen üblicherweise leichter als die Wahrscheinlichkeit zu berechnen, dass dieser Fall eintritt. Dazu geht man davon aus, dass das betrachtete Risiko innerhalb des Geltungsbereichs anfällt, und berechnet die verschiedenen Faktoren, aus denen dann eine Gesamtsumme berechnet werden kann. Bei diesen Faktoren kann es sich um einen Produktionsausfall handeln mit direkten Kosten, die entstehen oder der Ausfall der Telefonanlage im Direktmarketing, wobei man in diesem Fall z.B. den üblichen Umsatz über die Ausfallzeit für Berechnungen zugrunde legt.

10

10.8 Quantitative Darstellung von Risiken

Jede Entscheidung in einem Unternehmen folgt einer Abwägung zwischen Kosten und Nutzen. Die Festlegung von Maßnahmen, um ein Risiko auszuschalten oder zu reduzieren, macht dabei keine Ausnahme. Daraus lässt sich erkennen, wie wichtig es ist, Risiken in Zahlen und Fakten darstellen zu können. In den vorhergehenden Unterkapiteln wurden deshalb Richtlinien zur Klassifizierung beschrieben, der Zusammenhang zwischen Schutzbedarf und Kosten dargestellt und die Parameter Eintrittswahrscheinlichkeit und potenzieller Schaden eingeführt. Diese Faktoren bestimmen grundsätzlich die quantitative Wertigkeit eines Risikos. Für die Anpassung in ein betriebliches Umfeld müssen zudem Maßnahmen, die z.B. nach der letzten Risikobewertung eingeführt wurden, mit einberechnet werden, da sie die Eintrittswahrscheinlichkeit und/oder den potenziellen Schaden reduzieren können.

**Tipp**

Ein wichtiger Grundsatz des Risikomanagements lautet, dass für die Vermeidung eines Risikos nicht mehr Geld ausgegeben werden sollte, als das Risiko maximal bei Risikoeintritt kosten würde.

Die Daten und Fakten, die bislang im Laufe des Risikoprozesses gesammelt wurden, fließen nun in die mathematisch-statistische Berechnung und damit Darstellung des Risikos ein.

10.8.1 Grundlagen der Risikoberechnung

10

Kennzahlen dienen als Grundlage für die Berechnung von Risiken. Eintrittswahrscheinlichkeit, potenzieller Schaden und die erwarteten Kosten einer Maßnahme unter Einbezug des Restrisikos sind Variablen, die formal korrekt nur durch Ergebnisse aus der Ermittlung von Kennzahlen, die z.B. aus der Klassifizierung stammen, gefüllt werden können. Selbst wenn diese Werte durch Stufungen vereinfacht werden, sollte ein zumindest rudimentäres Ermitteln der Kennzahlen vorausgegangen sein.

Ein Risiko kann durch verschiedene Berechnungsarten ermittelt werden. Die wohl einfachste und damit am weitesten verbreitete sieht folgendermaßen aus:

$$\text{Risiko} = S_E * p_E$$

$$\text{Risiko} = (\text{Potenzieller}) \text{ Schaden} * \text{Eintrittswahrscheinlichkeit}$$

Der Charme dieses Ansatzes liegt in seiner Einfachheit. Insbesondere wenn es gilt, eine Betrachtung aus Sicht des IT-Risikomanagements für eine große Anzahl an Werten durchzuführen, erleichtert dieser Ansatz das Vorgehen. Auf der anderen Seite sind Maßnahmen, die zur Minderung des Risikos bereits getroffen wurden, nicht mit in die Berechnung eingeflossen. Daraus ergibt sich dann folgender, leicht veränderter Ansatz:

$$\text{Risiko} = (\text{Potenzieller}) \text{ Schaden} * (\text{Eintrittswahrscheinlichkeit} - \text{Maßnahmen})$$

Die dahinter steckende Aussage lautet: Die Eintrittswahrscheinlichkeit sinkt mit Anzahl und Qualität bereits ergriffener Maßnahmen. So wird eine Maß-



nahme »redundantes Netzteil einbauen« die Eintrittswahrscheinlichkeit senken und damit das Risiko des Ausfalls einer Serverhardware reduzieren.

$$\text{Risiko} = ((\text{Potenzieller Schaden} - \text{Maßnahmen}) * (\text{Eintrittswahrscheinlichkeit}))$$

Wird zumindest ein Teil des möglichen Schadens durch eine Cybercrime-Versicherung abgedeckt, dann vermindert sich der potenzielle Schaden durch die Deckungssumme.

Dadurch ergeben sich automatisch ein Risiko vor Ergreifung von Maßnahmen und eines danach. Dies ermöglicht es, Fortschritte in der Risikobehandlung darzustellen. Je mehr oder je bessere Maßnahmen implementiert werden, desto mehr werden diese zur Risikoverminderung beitragen und reduzieren dadurch das Risiko.

10

In der Praxis muss eine Reihe von grundsätzlichen Problemen immer im Hinterkopf behalten werden, um gegebenenfalls durch eine adäquate Maßnahme darauf zu reagieren:

- Der Wert »Eintrittswahrscheinlichkeit« hat einen sehr großen Einfluss auf den Wert des Risikos, und das, obwohl es sich dabei in den meisten Fällen um einen Schätzwert handelt. Ein Schätzwert, der z.B. aus Erfahrungen aus der Vergangenheit beruht, ist keine gute Kennzahl.
- Ein weiteres Problem liegt in der Berechnung: Extreme Werte wie eine sehr niedrige Schadenshöhe oder eine sehr hohe Eintrittswahrscheinlichkeit werden dadurch nicht sinnvoll dargestellt. Der Grund für das Problem liegt darin, dass die Relevanz nicht mit in die Berechnung einfließt. Aus diesem Grund wird ein sehr nebensächliches Problem mit sehr hoher Eintrittswahrscheinlichkeit ebenso hoch bewertet wie ein Katastrophenfall mit sehr niedriger Eintrittswahrscheinlichkeit.

Tipp

In Fällen eines sehr hoch zu erwartenden Schadens kann ein Risiko in der Praxis, ungeachtet einer eventuell nur sehr niedrigen Eintrittswahrscheinlichkeit, dennoch priorisiert betrachtet werden. Diese Vorgehensweise ist für alle Risiken zu empfehlen, deren Schadenseintritt existentielle Folgen verursachen würden. Typische Beispiele sind Vorkehrungen



für Katastrophen wie Brand, Wassereintritt oder die Erdbebenvorsorge. Auch wenn diese Ereignisse innerhalb des Betrachtungszeitraums bislang nicht aufgetreten sind, wird das Unternehmen dennoch eine weitgehende Vorsorge treffen müssen.

Eine Lösung wäre ein Ansatz, je nach potenzieller Schadenshöhe eine mathematisch modifizierte Formel zu nutzen. Dadurch würde die Vorgehensweise zwar deutlicher komplexer, die oben aufgeführten Probleme könnten sich dadurch aber lösen lassen.

10

Eine weitere Lösung wäre die Berücksichtigung eines weiteren Wertes, den der Relevanz (mit Werten zwischen 0 und 1) für das Unternehmen bzw. die Klassifizierungsstufe des gefährdeten Wertes. Die Höhe des Wertes »Relevanz« kann z.B. aufgrund eines Beschlusses durch die Unternehmensleitung getroffen werden, wie es bei Risikovorsorgekategorien wie »Schutz gegen einen kriegerischen Akt« oder »Schutz vor Flugzeugabsturz« häufiger der Fall ist. In diesen Fällen geht es auch um die Risikoaffinität des Unternehmens oder die Unternehmenskultur.

$$\text{Risiko} = (S_E * p_E * \text{Relevanz}) - \text{Maßnahmen}$$

Zusammengefasst lässt sich sagen, dass die Herausforderung in der Beifügung von Risiken darin liegt, einen möglichst formalisierten, objektiven Berechnungsansatz zu finden. Die beiden Schlüsselwerte sind dabei die erwarteten Kosten im Fall des Eintretens des Schadens und die Eintrittswahrscheinlichkeit. Durch die Entzerrung des Wertes »Risiko« in zwei oder gar drei Werte, die jeweils mit Zahlen zu untermauern sind, wird die Berechnung eines Risikos transparenter. Hilfreich ist auch, dass die Faktoren »erwarteter Schaden« und »Eintrittswahrscheinlichkeit« häufig von verschiedenen Parteien definiert werden müssen, Ersterer vom Eigentümer der betroffenen Daten, Letzterer beispielsweise von der IT-Abteilung.

10.8.2 Risikoberechnung im Beispiel

Ein weiteres Mal wird das Beispiel »Virenscanner« bemüht – dieses Mal, um daran eine beispielhafte Vorgehensweise aufzuzeigen. Der Sachverhalt in unserem Beispiel stellt sich folgendermaßen dar: In der Firma ABC sind auf allen Arbeitsplatzrechnern Virenscanner installiert. Auf den Servern dagegen



hat man dies unterlassen, da die VirensScanner auf den PCs ausreichen sollten. Nach einiger Zeit stellt sich allerdings heraus, dass trotz der gesicherten Rechner immer wieder Viren und Trojaner im Netzwerk auftauchen und dort massiv Störungen verursachen. Die Implementierung der Maßnahme »Installation VirensScanner auf Datenservern« soll nun Abhilfe schaffen. Um den Erfolg zu messen und danach eine laufende Überprüfung zu gewährleisten, wurde eine Matrix zur Berechnung erstellt.

Der Manager IT-Security bekommt nun die Aufgabe übertragen, das Risiko darzustellen und nachzuweisen, dass die eingeführten Maßnahmen zum Erfolg führen.

Ermittlung einer Kennzahl

Nach Gesprächen mit der zuständigen IT-Abteilung sind sich die Beteiligten sicher, dass Applikationen und Dateien auf den Servern von Viren befallen sind. Da diese oft direkt vom Server aus aufgerufen werden, schaffen es einige davon, sich am VirensScanner, der auf den Arbeitsplatzrechnern installiert ist, vorbei zu verbreiten bzw. allgemeiner ausgedrückt: ihre Schadensroutine auszuführen. Die Installation eines VirensScanners auf den File-, Druck- und Mailservern ist also eine logische Konsequenz. Um im Nachhinein eine Verbesserung der Situation nachweisen zu können, muss der Grad der Verseuchung vor der Installation erfasst werden.

Alle von der Antivirensoftware gefundenen Viren werden in einer zentralen Datenbank dokumentiert. Die Auswertungen reichen einige Monate zurück und sind lückenlos. Also wird die Kennzahl als »Summe aller innerhalb eines Jahres gefundene Schadsoftware geteilt durch 365 Tage« definiert. In unserem Fall wurden 5110 Viren, Trojaner und Würmer gefunden, das ergibt 14 pro Tag. Diese Kennzahl stellt den Basiswert für eine spätere Überprüfung der dann neuen Ist-Situation dar.

Risikodarstellung vor Einführung einer Maßnahme

Die Firma ABC geht einen sehr pragmatischen und überschaubaren Weg, wenn es um die Darstellung eines Risikos geht. Die Gründe dafür liegen vor allem darin, dass man sich davon eine Durchgängigkeit verspricht, die auch mit kleinem Budget und wenigen Ressourcen durchzuhalten ist. Abgeleitet vom NPLF-Modell, das die Stufen *not achieved*, *partially achieved*, *largely achieved* und *fully achieved* kennt, werden in Firma ABC auch die Risiken, was den



Schaden und was die Eintrittswahrscheinlichkeit angeht, in vier Stufen bewertet:

- Niedrig (Wert 1)
- Mittel (Wert 2)
- Hoch (Wert 3)
- Sehr hoch (Wert 4)

Auf Basis von insgesamt 1000 PCs ist die Anzahl von 14 Infektionen täglich eine relativ hohe Zahl, und der IT-Verantwortliche definiert die Eintrittswahrscheinlichkeit als hoch. Den dabei entstandenen Schaden stuft er auf Basis der im letzten Jahr aufgrund von Schadsoftware ausgefallenen Arbeitsstunden als mittel ein. Diesen beiden Einstufungen sind die numerischen Werte 3 für hohe Eintrittswahrscheinlichkeit und 2 für mittleren Schaden hinterlegt worden. Diese Definition liegt als unternehmensweit gültige Regelung vor. Nach der Berechnungsmethodik

$$\text{Risiko} = (\text{Potenzieller}) \text{ Schaden} * \text{Eintrittswahrscheinlichkeit}$$

liegt damit ein Risiko vor, das mit $(2 * 3) = 6$ Punkten bewertet werden muss. Hinterlegt man noch die in der Klassifizierungsmatrix festgelegte Summe an Geld, die einem potenziellen Schaden von 2 entspricht, dann liegt eine Bewertung auf Basis von Euro vor. Dieses bewertete Risiko bezeichnet man als »Risikowert«.

Risiko nach Einführung einer Maßnahme

Die Viren pro PC vor Umsetzung der Maßnahme »Installation Virensanner auf dem Server« sind ermittelt. Nun kann die Maßnahme umgesetzt werden, um im Anschluss daran die Kennzahl neu zu erfassen. Angenommen, die Anzahl an Schadsoftware hat sich auf einen Fund pro Tag reduziert. Ausgehend von einem Fund pro Tag würde dann die Eintrittswahrscheinlichkeit von hoch nach niedrig fallen. Dementsprechend sinkt der Risikowert deutlich – von 6 auf 2 Punkte. Für den zuständigen Manager würde dies genügen, um die Reduzierung des Risikos nachvollziehbar darzustellen.

10.8.3 Risikomatrix

Die Risikomatrix stellt eine häufig eingesetzte Visualisierungstechnik dar. Durch ihre Anordnung wird der Zusammenhang von Eintrittswahrschein-



lichkeit, möglichem Schaden und der daraus folgenden Klassifizierung auf einen Blick deutlich. Risiken lassen sich direkt entsprechenden Feldern zuordnen, um dann die jeweilige Gewichtung abzulesen.

		Eintrittswahrscheinlichkeit				
		Unwahr-scheinlich	Sehr selten	Selten	Oft	Sehr oft
Potentieller Schaden	Sehr niedrig	Sehr klein	Sehr klein	Sehr klein	Klein	Mittel
	Niedrig	Sehr klein	Sehr klein	Klein	Mittel	Mittel
	Mittel	Sehr klein	Klein	Mittel	Hoch	Hoch
	Hoch	Klein	Mittel	Hoch	Sehr hoch	Sehr Hoch
	Sehr hoch	Hoch	Hoch	Sehr hoch	Kata-strophe	Kata-strophe
	Existentiell	Sehr hoch	Sehr hoch	Kata-strophe	Kata-strophe	Kata-strophe

Abbildung 10.22: Risikomatrix

10

Eine Richtlinie zur Risikobehandlung könnte, basierend auf einer Risikomatrix, folgende Regelungen festlegen:

- Wird ein Risiko als »Niedrig« (N) eingestuft, so sind im Allgemeinen keine besonderen Maßnahmen erforderlich.
- Risiken der Stufe »Mittel« (M) erfordern die Ergreifung von Maßnahmen, um das Risiko nachhaltig zu reduzieren. In diesen Fällen handelt es sich oft um technische Vorkehrungen, wie sie z.B. in den Grundschutzhandbüchern des BSI beschrieben sind.
- Risiken der Einstufung »Hoch« (H) erfordern Maßnahmen, die über den Rahmen des Grundschutzes nach BSI hinausgehen. Oft werden auch Änderungen in Prozessen erforderlich, um das Risiko wieder auf ein akzeptables Niveau zu senken.



- Risiken der Stufe »Sehr hoch« erfordern sofortigen Handlungsbedarf. In diesen Fällen ist sowohl die mögliche Schadenshöhe als auch die Eintrittswahrscheinlichkeit und damit der Risikowert untragbar hoch. Wenn erforderlich, müssen Prozesse angepasst und Maßnahmen umgesetzt werden, um das Risikoniveau zumindest auf die Stufe »Hoch« zu senken.

Die Risikomatrix spiegelt die Risiken der Werte im Unternehmen wider und kann daher stark unterschiedlich ausgeprägt sein. Da es keine normierte Vorgabe gibt, kann sie für ein Unternehmen sehr flexibel definiert werden.

10.8.4 Risikokatalog

10

Die einheitliche Darstellung und Beschreibung von Risiken erfolgt in Risikokatalogen. Im Grunde handelt es sich dabei um ein Verzeichnis der Risiken inklusive der Parameter und der Beschreibung von Maßnahmen sowie deren Fortschritt. Diese Parameter beschreiben ein Risiko, und gleichzeitig ermöglichen sie es, ein Risiko einzuordnen und damit mit anderen, gleichartigen Risiken vergleichbar zu machen. Häufig beziehen sich die beschriebenen Risiken direkt auf die Maßnahmen aus Anhang A der ISO 27001.

Innerhalb eines Risikokatalogs sollten für jedes Risiko die folgenden Attribute beschrieben werden:

- **Risikoname:** Inhalte eines Risikos werden sich im Laufe der Zeit genauso verändern wie eingeführte Maßnahmen oder die Risikobewertung. Aus diesem Grund sollten keine weiteren Parameter Bestandteil des Risikokatalogs sein.
- **Risikoart:** Die Kategorisierung eines Risikos ist abhängig vom Ordnungskriterium Risikoart. Beim Aufbau eines IT-Risikomanagements sollte man also einige Zeit darauf verwenden, die möglichen Risikoarten zu definieren.
- **Risikobeschreibung:** Die Beschreibung des Risikos ist wichtig, da sie Rückschlüsse auf die ermittelten Bedrohungen, Schwachstellen und die Bewertung zulässt. Bietet der Risikokatalog die Möglichkeit einer Volltextsuche, so kann auch hierüber nach Stichworten gesucht und das Risiko kategorisiert werden.
- **Verantwortliche Stelle und verantwortliche Person**
- **Bedrohung:** Zur besseren elektronischen Verarbeitung ist es sinnvoll, Bedrohungarten im Vorfeld zu definieren und in einem eigenen Katalog ab-



zulegen. Dadurch kann in dieser Spalte eine direkte Zuordnung zu einem oder mehreren Bedrohungen stattfinden. Da kein Freitext verwendet wird, kann so z.B. später eine Auswertung erstellt werden, welche Risiken mit Bedrohung n verknüpft sind.

- **Möglicher Schaden für einen Unternehmenswert:** Ein Risiko kann mehrere Systeme bzw. Werte beeinträchtigen. In dieser Spalte wird für jeden betroffenen Wert der Schaden anhand einer definierten Skala festgestellt. Die Informationen zu den Werten werden in einem separaten Assetmanagement geführt. An dieser Stelle genügt wiederum ein Link auf den entsprechenden Eintrag.
- **Eintrittswahrscheinlichkeit:** Auch die Eintrittswahrscheinlichkeit wird in Form einer definierten Skala festgestellt. Die Angabe bezieht sich dabei auf die Anzahl der Vorkommnisse innerhalb eines definierten Zeitraums.
- **Maßnahmen:** Die zur Risikobehandlung definierten Maßnahmen können nun aufgeführt werden. Auch hier empfiehlt sich ein Link auf einen separat angelegten Katalog an Maßnahmen, die wiederum am besten von einer normierten Quelle wie z.B. der ISO 27001 oder den BSI-Grundschutz-Katalogen abgeleitet sind.
- **Status der Maßnahmen**
- **Risikoberechnung/Restrisikoberechnung:** Falls vorgesehen, kann auf Basis der vorliegenden Parameter eine Risikoberechnung stattfinden, die es ermöglicht, die erfassten Risiken entsprechend zu bewerten.

Verwenden Sie mehrere Kataloge in mehreren Bereichen im Unternehmen, dann ist es wichtig, nicht nur auf übereinstimmende Kriterien zu achten, sondern auch darauf, dass sich die Risiken bzw. die betrachteten Werte nicht überschneiden. Es ist grundsätzlich wahrscheinlich, dass eine Maßnahme Einfluss auf mehrere Risiken hat, und wenn dieser risikomindernde Einfluss nicht erfasst wird, dann wird die Gesamtbetrachtung zunehmend inkonsistent. Die Zusammenführung mehrerer Kataloge wird dementsprechend eine Darstellung der Verflechtung der Risiken untereinander voraussetzen. Dazu müssen die Einflüsse der Risiken aufeinander bestimmt werden. Diese Einflüsse können sich risikomindernd oder risikoverstärkend auswirken. Insbesondere die Risiken, die risikoverstärkend auf andere Risiken einwirken, müssen entsprechend gekennzeichnet werden.



10.9 Risikobehandlung

Auf das Risiko »Ein Virus löscht Daten auf dem Datenserver« kann entweder pauschal reagiert werden oder aber es findet eine Abwägung aller Risiko-parameter statt, die zu einer individuellen, auf den einzelnen Wert bezogenen Entscheidung führt. Im vorliegenden Fall wird vermutlich pauschal das im Unternehmen eingesetzte Antivirenprogramm installiert, ohne dass eine weitere Untersuchung des Risikos stattfindet. Das liegt vor allem daran, dass eine entsprechende Anwendung im Unternehmen bereits existiert sowie vermutlich bereits lizenziert ist und die Installation eine Tätigkeit darstellt, die schnell und effizient vonstatten geht, ohne dass dadurch weitere Risiken entstehen. Die Erfahrung mit vielen anderen Installationen erlaubt in diesem typischen Fall eine solche Vorgehensweise.

10

Handelt es sich aber um den ersten Server und wird eine Antivirensoftware benötigt, die nicht bereits im Unternehmen vorhanden ist, so ist der Fall anders gelagert. Es muss zwischen den Kosten des Erwerbs und der Installation gegenüber dem Risiko, nichts zu installieren, abgewogen werden. Es kann also sehr wohl sein, dass die Kosten einer Installation höher sind als die, das Risiko zu tragen. In diesem Fall würden der Erwerb von Software und die Reduzierung des Risikos betriebswirtschaftlich keinen Sinn machen.

In beiden Fällen handelt es sich um das gleiche Risiko auf Basis der gleichen Unternehmenswerte und führen zu einer jeweils unterschiedlichen Risikobehandlung. Dadurch wird deutlich, dass mehr Parameter bedacht werden müssen als nur diejenigen, die zur Quantifizierung des Risikos erforderlich sind.

Bevor nun eine Entscheidung getroffen wird, ob ein Risiko durch die Umsetzung von Maßnahmen behandelt werden soll, müssen die Kriterien für eine solche Entscheidung festgelegt werden. Im Grunde geht es um die Frage, ob eine Maßnahme angemessen ist, also ob der Nutzen und die Kosten in einem Verhältnis stehen, das das Unternehmen anstrebt. Die verschiedenen Schritte im Prozess des Risikomanagements, die in den letzten Kapiteln beschrieben wurden, liefern den Input für diese Entscheidung.

Generell gesehen gibt es mehrere Möglichkeiten, mit einem Risiko umzugehen. Gängig sind vor allem die folgenden:



- Ein Risiko kann durch Einführung entsprechender Maßnahmen reduziert werden.
- Ein Risiko kann akzeptiert werden.
- Ein Risiko kann vermieden werden, indem Prozesse vermieden werden, die zu seinem Eintreten führten.
- Ein Risiko kann auf einen Dritten verlagert werden. Dies kann z.B. durch den Abschluss einer entsprechenden Versicherung geschehen.

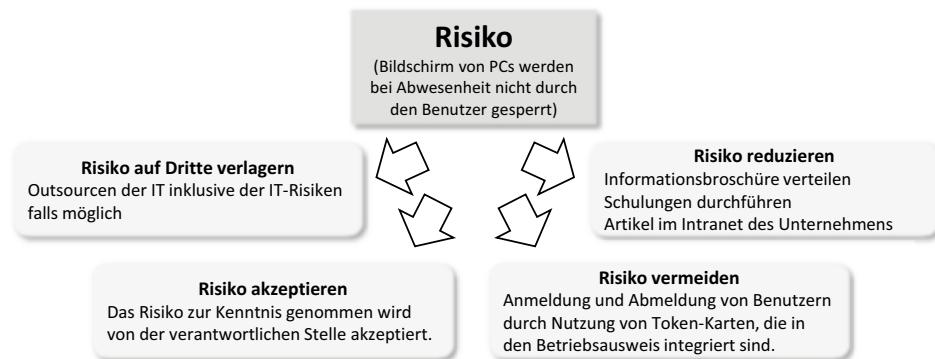


Abbildung 10.23: Alternativen der Risikobehandlung

Vollständige Sicherheit und damit auch die vollständige Ausschaltung aller Risiken existiert nicht. Alle Tätigkeiten des Managers IT-Security dienen dazu, sich diesem Optimum möglichst weit anzunähern. Je weniger Risiken einen Prozess oder ein IT-System und damit die dadurch verarbeiteten Daten gefährden, desto leichter ist die Reduzierung dieser wenigen Risiken. Je komplexer aber ein System wird, desto mehr Unwägbarkeiten in Form von gegenseitigen Abhängigkeiten sind vorhanden.

In beiden Fällen gilt das Prinzip, dass ein ausgewogenes Verhältnis von investiertem Kapital und erreichtem Sicherheitsgrad angestrebt werden sollte. Der angestrebte Sicherheitsgrad, der aus den entsprechenden Richtlinien ableitbar ist, sollte erreicht werden, ohne dass die Kosten den Nutzen des damit zu erreichenden Sicherheitsgrads übersteigen. Das Ziel des Risikomanagements ist es nun, neben der Schaffung von Transparenz diesen Zielkorridor zu finden und die dafür erforderlichen Maßnahmen zu definieren.

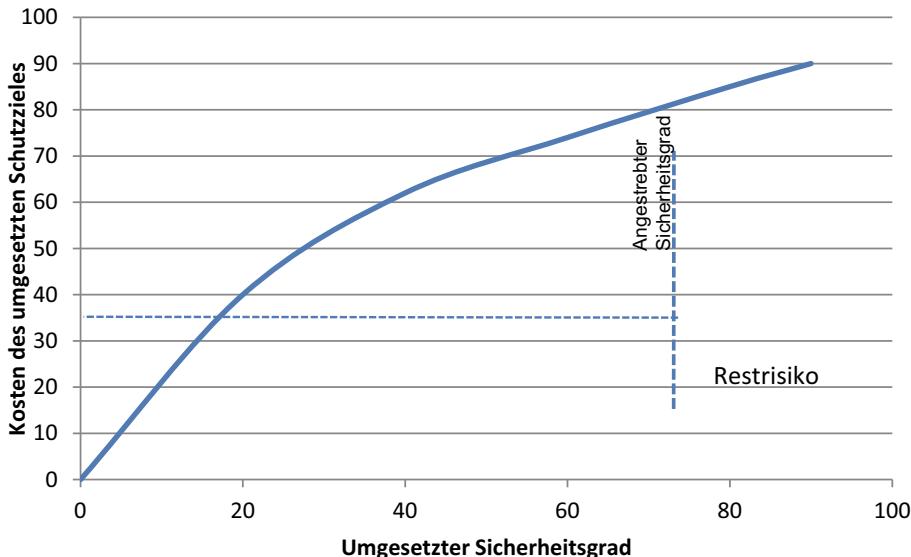


Abbildung 10.24: Beziehung zwischen Kosten und Sicherheitsgrad

Es existiert ein Zusammenhang zwischen Steigerung des Sicherheitsgrads und Senkung des Leistungsgrads der Datenverarbeitung. Je mehr Maßnahmen zum Informationsschutz eingeführt werden, desto mehr kann die Leistungsfähigkeit von IT-Systemen darunter leiden. Das betrifft nicht nur den Benutzer, der unter Umständen einmal pro Woche sein 20-stelliges Passwort vergisst, sondern auch den Administrator, der bei zu aufwendig gestalteten Notfallplänen aufgrund ständigen, detaillierten Nachdokumentierens seine Wartungsfenster nicht einhalten kann. Auch diese Folgen können monetär bewertet werden. Da dies aber im Rahmen des Risikomanagements oft nicht geschieht, fällt es bei der abschließenden Risikobehandlung meist unter den Tisch. Aus diesem Grund sollte es zumindest in der letzten Phase der Risikobehandlung betrachtet werden.

10.9.1 Risiko akzeptieren

Die Entscheidung, ein Risiko zu akzeptieren und keine weiteren Maßnahmen zu implementieren, sollte auf den Richtlinien zur Risikobehandlung basieren. Diese Richtlinien definieren, welche Kriterien herangezogen werden, um die Entscheidung zur Risikobehandlung zu treffen. Gute Richtlinien in diesem Bereich erkennt man daran, dass eine klare und stringente Argumenta-



tion und Entscheidungshilfe vorhanden ist, die es den jeweiligen Vorgesetzten erlaubt, eine nachvollziehbare Entscheidung zu treffen.

Wichtig

Die Akzeptanz eines Risikos ist eine Entscheidung, die genauso wie die Festlegung von Maßnahmen dokumentiert werden muss.

Einem Risiko steht immer auch eine Chance entgegen, ansonsten wäre es nicht sinnvoll, ein Risiko im Unternehmensumfeld zu akzeptieren. In den Fällen, in denen diese Chance quantifizierbar ist, fällt es einem Entscheider leicht, dieses Ergebnis dem Risiko gegenüberzustellen und daraus eine Entscheidung abzuleiten. In den allermeisten Fällen allerdings ist es nicht möglich, die schwer zu fassende Größe »Chance« in einen vergleichbaren Zusammenhang zu setzen. Aus diesem Grund wird die Entscheidung, ein Risiko bzw. Restrisiko zu akzeptieren, darauf beruhen, inwieweit von den Schutzziehen Vertraulichkeit, Verfügbarkeit und Integrität abgewichen wird, falls das Risiko eintritt. Es handelt sich also um eine Entscheidung, die darauf gründet, ob mögliche Konsequenzen für das Unternehmen akzeptabel sind oder nicht.

10

10.9.2 Risiko reduzieren

In den meisten Fällen wird die Risikobehandlung darin bestehen, ein erkanntes und klassifiziertes Risiko zu verringern. Dies erfolgt durch die Auswahl und die Umsetzung von Maßnahmen. Ziel ist es, das Risiko auf ein akzeptables Niveau zu senken.

Die Auswahl von Maßnahmen mit dem Ziel, das Risiko zu vermindern, basiert auf Kriterien, die im Rahmen des Risikoerfassungs- und -bewertungsprozesses ermittelt wurden. Im Gegensatz zur Risikoakzeptanz und zur Risikovermeidung erfolgt die Reduzierung graduell. Das bedeutet, dass jeweils abgewogen werden muss, ob die Implementierung einer Maßnahme zu einer Reduzierung führt, die sich lohnt.

Einflussfaktoren bei dieser Einschätzung sind unter anderem

- die Kosten der Einführung der Maßnahme
- Nebeneffekte wie z.B. durch die Implementierung neu entstehende Risiken oder die Erhöhung von bestehenden Risiken. So kann die Umsetzung



- von verschärften Regeln auf der Firewall zu einer Nichtverfügbarkeit von Applikationen führen
- Verpflichtungen gegenüber Kunden, Lieferanten oder öffentlichen Stellen
 - die Einhaltung von Gesetzen und Verordnungen
 - Zugriffszeiten und allgemein technische Aspekte, die auf die Fähigkeit zielen, IT-Dienstleistungen zu erbringen

Neben der Auswahl von Maßnahmen ist jeweils auch der Grad der Umsetzung zu bestimmen. So kann es zu einem günstigeren Verhältnis von Geschäftsbetrieb und Risiko führen, wenn eine Maßnahme nur eingeschränkt umgesetzt wird. Auf der anderen Seite können häufig zukünftige Kosten eingespart werden, wenn durch Sicherheitsmaßnahmen Regulierungen vorgenommen werden, die auch erst zukünftig aktuell werdende Sicherheitsaspekte abdecken.

10

10.9.3 Risiko vermeiden

In Fällen, in denen ein Risiko als hoch eingeschätzt wird, die Implementierung von Maßnahmen aber unwirtschaftlich erscheint oder aus anderen Gründen nicht ratsam ist, existiert eine weitere Alternative, und zwar die, das Risiko zu vermeiden.

Dies kann geschehen, indem Prozesse, die das Risiko verursachen, verändert oder indem alternative Prozesse oder technische Methoden implementiert werden. Ein häufiger Fall der Risikovermeidung ist dann gegeben, wenn Risiken durch Gefahren ausgelöst werden, die schwer beherrschbar sind. Dazu gehört z.B. Hochwasser, das den Betrieb eines Serverraums bedroht. In diesem Fall wäre ein Umzug der Räumlichkeiten in das fünfte Obergeschoss ein Weg, das Risiko zu vermeiden.

10.9.4 Risiko auf Dritte verlagern

Die Verlagerung eines Risikos bzw. Restrisikos auf einen Dritten, z.B. durch den Abschluss einer Cybercrime-Versicherung, entlastet das eigene Unternehmen von den Folgen des möglichen Eintretens eines Schadenfalls. Die Entlastung bezieht sich vorrangig auf die finanzielle Seite eines Vorfalls. Nichtverfügbarkeit der Internetpräsenz als Beispiel wird trotz einer Versiche-



rung, die für finanzielle Schäden aufkommt, dem Unternehmen angelastet werden und kann zu einem Imageverlust führen, der durch eine Versicherung üblicherweise nicht vollständig abgedeckt werden kann.

Seit es Versicherungen gibt, werden Risiken verlagert. Im Umfeld der IT gehören Versicherungen gegen die Risiken der höheren Gewalt wie Feuer oder Wasser zu den gängigsten. Aber auch die Absicherung gegen technische Schäden an IT-Equipment ist üblich. Diese Risiken haben gemeinsam, dass sie oftmals genau kalkulierbar sind. Eine Regulierung über den Neuwert von Computern ist zu berechnen. Risiken für den Geschäftsbetrieb wie z.B. bei einem Internethändler, der sich gegen das Risiko eines Ausfalls seiner Internetanwendung versichern möchte, sind dagegen bereits sehr viel schwieriger einzuschätzen. Dies beginnt bei der Risikoeinschätzung und endet bei der Festlegung der Schadenssumme. Aus diesem Grund sind Versicherungen in diesem Umfeld deutlich seltener.

10

10.10 Maßnahmen definieren

Maßnahmen dienen der Reduzierung oder gar Ausschaltung eines Risikos und beziehen sich auf einen Unternehmenswert. Die Frage, ob technische oder organisatorische Maßnahmen erforderlich sind, wird von den Ergebnissen der Risikoanalyse abgeleitet.

Tipp

Vor der Implementierung neuer Maßnahmen sollte überprüft werden, ob nicht bereits realisierte Maßnahmen erweitert bzw. optimiert werden können. Häufig reicht es bereits, Regelungen hinsichtlich bestehender Maßnahmen zu konkretisieren bzw. zu ergänzen.

Die Frage nach der jeweils geeigneten Maßnahme nachhaltig richtig zu beantworten, setzt ein gewisses Maß an Kontrollfunktionalitäten voraus, mit denen die Wirksamkeit von Maßnahmen überprüft werden kann. Zu diesem Zweck werden Kennzahlen eingesetzt, um Zahlenmaterial vor der Einführung, während des Betriebs und nach einer Verbesserung bezüglich Fortschritte oder Rückschritte zu erfassen.



Komplexe Maßnahmen, interagierende Maßnahmen oder solche, die auf verschiedene Bereiche Auswirkungen haben, müssen einer systematischen Umsetzungsplanung unterworfen werden.

10.10.1 Maßnahmentypen

Maßnahmen, die zur Reduzierung eines Risikos eingesetzt werden können, stammen zumeist aus dem technischen Bereich. Viele der Arbeitsabläufe innerhalb der IT z.B. dienen primär oder sekundär der Verminderung eines Risikos. Dazu zählt die komplette Bandbreite der Serviceaufgaben von IT-Support, IT-Hotline sowie die Arbeit in Projekten bis hin zur System- und Softwareadministration. Dabei geht es nicht nur um die klassischen Aufgaben der IT-Security wie die Installation von Updates oder eines Antivirenprodukts. Auch Methoden zur Standardisierung oder automatisierte Vorgänge wie die Anlage eines Benutzers können direkt zu den gelebten Maßnahmen gezählt werden. Zur Gruppierung von Maßnahmen bietet es sich an, sich an der ISO-Kategorisierung zu orientieren. In ISO 27002 findet eine solche Gruppierung statt. In der ISO 27001 werden zudem Maßnahmenziele, hier als Gruppierung zu verstehen, sowie konkrete Maßnahmen dargestellt. Die Grundschutz-Kataloge des BSI bieten als Ergänzung zu den Maßnahmenzielen der ISO 27001 und ISO 27002 viele weitere konkrete Maßnahmen. An dieser Ordnung orientieren sich viele Unternehmen und verzichten bewusst darauf, von Grund auf eigene Maßnahmenkataloge zu entwickeln.

Die Maßnahmen aus Anhang A der ISO 27001 unterteilen sich, grob ausgedrückt, in organisatorische und in technische Maßnahmen. Weitere Unterschiede liegen darin, dass es sich zum Teil um zentrale Themen handelt und zum Teil um Einzelmaßnahmen, die in jeder Niederlassung eines Unternehmens individuell betrachtet werden müssen. So beschäftigt sich Abschnitt 5 des Anhangs A der ISO 27001 mit Themen wie z.B. der Sicherheitsrichtlinie. Diese wird in den meisten Fällen entweder für das gesamte oder aber zumindest für einen großen Teil des Unternehmens zuständig sein. Aus diesem Grund wird sich eine zentrale Stelle um die Erstellung und Pflege dieses Dokuments kümmern. Verantwortliche in anderen Unternehmensteilen werden, wenn sie nicht an diesem Entstehungsprozess teilhaben, keinen Einfluss darauf haben, ob das Dokument existiert oder nicht.

Folgende Gliederung der Maßnahmen und daraus zu folgernde Interviewpartner sind denkbar:



- Globale Maßnahmen: Dabei handelt es sich vor allem um Dokumente, die einen unternehmensweit nutzbaren Charakter haben. Das sind z.B. die Basisrichtlinien und Richtlinien zum generellen Umgang mit Informationen. Kapitel 5 des Anhangs A der ISO 27001 besteht in weiten Teilen aus globalen Maßnahmen. Dazu kommen Maßnahmen, die unternehmensweit umgesetzt werden sollten, um auf ein angestrebtes Sicherheitsniveau zu kommen. Dazu zählen bereits Maßnahmen wie der Einsatz von Virenscannern oder die Verschlüsselung kritischer Daten.
- Lokale Maßnahmen: Alle Maßnahmen, die für jeden einzelnen Unternehmensstandort von Relevanz sein können, gelten als lokale Maßnahmen. Diese Maßnahmen entstehen zumeist aufgrund einer nicht standardisierten Umsetzung von IT-Infrastrukturthemen oder aufgrund von lokalen Vorgaben.

Die Unterteilung nach Maßnahmentypen ist aus mehreren Gründen hilfreich. Zum einen wird dadurch eine Zuordnung von Zuständigkeiten erleichtert, und zum anderen können Auswertungen getrennt nach Fortschritten im globalen und im lokalen Bereich dargestellt werden. Dadurch werden die einzelnen Unternehmensstandorte von vielen Anforderungen entlastet, zu deren Umsetzung sie unter Umständen überhaupt nicht beitragen können.

10.10.2 Individuelle Maßnahmenkataloge

Je näher man sich an unternehmensübergreifenden und international akzeptierten Maßnahmenkatalogen orientiert, desto eher ist die Vergleichbarkeit mit anderen Unternehmen gegeben und desto einfacher wird es häufig sein, diese Kataloge unternehmensweit durchzusetzen. Dabei kann es natürlich sinnvoll sein, Kataloge durch eigene Maßnahmenziele und Einzelmaßnahmen zu ergänzen. Aus diesen Ergänzungen ergeben sich dann individuelle Maßnahmenkataloge.





11 Sicherheitsmonitoring

11.1 Kapitelzusammenfassung

Die Überwachung von IT-Systemen und Applikationen ist ein zentrales Gebiet der IT-Security und der IT im Allgemeinen. Es bietet Hilfestellungen für eine ganze Reihe von Aufgaben und unterstützt das Management von Sicherheitsereignissen ebenso wie das IT-Notfallmanagement. Es dient der Unterstützung der klassischen drei Schutzziele, der Wahrung von Vertraulichkeit, Integrität und Verfügbarkeit. Das Schutzziel der Belastbarkeit aus der EU-DSGVO oder weitere Schutzziele wie die Authentizität können über entsprechende Überwachungen beteiligter IT-Systeme und Applikationen integriert werden.

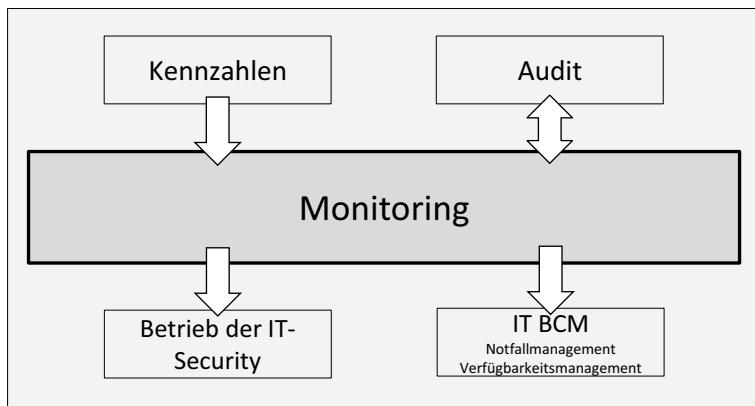


Abbildung 11.1: Primäre Abhängigkeiten von anderen Themen der IT-Security

Ein Hauptziel der IT-Security ist die Schaffung von Transparenz, und diese wird zu einem großen Teil durch die Auswertungen des Monitorings erzeugt. In diesem Kapitel werden die Grundzüge und wichtigsten Rahmenbedingungen für den Einsatz entsprechender Werkzeuge vorgestellt.



Die Top-5-Fragen zum aktuellen Kapitel:

- Ist ein Monitoring von Sicherheitsereignissen und der wirksamen Umsetzung von IT-Security-Maßnahmen, wie Patchmanagement, implementiert?
- Werden kritische IT-Systeme durch ein aktives Monitoring überwacht?
- Findet eine Alarmierung statt, wenn der Ausfall von IT-Systemen durch das Monitoring entdeckt wird?
- Werden Daten aus dem Monitoring in eine Langzeitspeicherung übernommen, um später mittelfristige Entwicklungen nachzubilden zu können? Die im Rahmen des Monitorings erfassten Daten können dem Sizing von Hardware genauso dienen wie dem Verfügbarkeitsmanagement oder der Identifizierung von Risiken.
- Werden Schwachstellen von Betriebssystemen und Applikationen systematisch erfasst, in geeigneter Form dargestellt und abgearbeitet?

11

11.2 Einführung

Zu wissen, was mit den Daten des Unternehmens geschieht, in welchem Zustand sich die IT-Systeme befinden, welche offenen Schwachstellen es gibt, und diese Fakten auch darstellen, nachverfolgen und dokumentieren zu können, ist die Aufgabe des Monitorings. Dies dient nicht nur den Zwecken der IT-Security und dem Betrieb der IT. Darüber hinaus hat das Unternehmen die Pflicht, Nachweise zu erbringen, was mit personenbezogenen Daten passiert und wie der aktuelle Status der Schutzmaßnahmen aussieht. Aus diesen Aufgaben lassen sich zwei Kernbereiche des Monitorings ableiten:

- Die Verbindung des Monitorings zum IT-Security-Management kommt über mehrere gemeinsame Zielsetzungen zustande. So ist Monitoring ein wichtiger Bestandteil des IT Continuity Managements, da ein zeitnahe Reagieren auf Störfälle nur durch zielgenaues Feststellen von Problembe reichen möglich ist. Auch dienen Fehlermeldungen von IT-Systemen wie Plattensystemen oder auch von Applikationen dazu, möglichst weit im Voraus mögliche Störungen aufzudecken. Damit unterstützt das Monitoring den Betrieb von IT-Systemen auf Ebene der Hard- und Software und dient in erster Linie dazu, die Umsetzung des Schutzzieles »Verfügbarkeit« zu verfolgen.



- Ein weiterer Kernbereich des Monitorings besteht darin, die Vertraulichkeit und Integrität von Daten zu unterstützen. Hier kommen sogenannte Security-Information-and-Event-Management-(SIEM-)Systeme zum Einsatz. Ein SIEM dient dazu, dem IT-Security-Management ein einheitliches und möglichst vollständiges Lagebild der Sicherheit im Unternehmen zu geben. Dieses Bild umfasst auf der einen Seite aktuelle Kennzahlen zu Bereichen wie die Anzahl nicht gepatchter Systeme, unverschlüsselter Laptops oder veralteter Betriebssysteme und auf der anderen Seite aktuelle Meldungen wie durch Intrusion-Detection-Systeme oder Firewalls gemeldete Sicherheitsverstöße. Das so erzeugte Lagebild wird damit zu einer zentralen Kontrollinstanz.

Die Erweiterung eines SIEM wird dann erforderlich, wenn es darum geht, Ereignisse in Echtzeit zu erkennen und zeitnah darauf zu reagieren. In diesem Fall wird in Unternehmen ein Security Operation Center (SOC) aufgebaut. Die Infrastruktur, die dazu genutzt wird, greift hierbei entweder direkt auf die Originalquellen zu oder bedient sich der Datenbank eines SIEM.

Ein SOC, das rund um die Uhr arbeiten soll, wird häufig in Form einer Sicherheitsdienstleistung eingekauft. In diesem Fall ist es entscheidend, geeignete Schnittstellen zwischen dem externen Dienstleister und der eigenen IT-Security-Abteilung aufzubauen. Entsprechend hoch klassifizierte Sicherheitsereignisse müssen im Notfall auch am Wochenende durch das Unternehmen abgearbeitet werden können.

Eine weitere Herausforderung ist es, sicherzustellen, dass die Einklassifizierung gemeldeter Ereignisse stimmig ist. Manche Sicherheitsvorkommnisse sind dringender als andere und das hängt unter anderem vom Zweck eines Unternehmens ab. Nutzt man externe Dienstleister, dann ist ein Zeitraum einzuplanen, der dazu dient, diese Abstimmung vorzunehmen.

In den folgenden Unterkapiteln wird das Hauptaugenmerk auf das Monitoring an sich gelegt. Dabei kann es sich um die Überwachung von Sicherheitslogs handeln oder um die Überwachung der Verfügbarkeit von IT-Systemen. Ein Beispiel dafür wäre die Überwachung von Zugriffen auf Datenserver. Werden verdächtige Zugriffe getätigt, wird Alarm ausgelöst. Abgesehen davon, dass die dann benachrichtigten Personen oft aus einem anderen Bereich des Unternehmens kommen als der IT-Security, z.B. aus dem Support oder



dem Bereich der Administratoren, ist diese Art von Alarmierung aus Sicht der IT-Security mit denen von anderen Sicherheitsereignissen gleichzusetzen, die in einem CSIRT auflaufen.

Das Aufspüren von Sicherheitsereignissen durch ein Monitoring-System lässt sich wiederum mit Verhaltensmustern von Benutzern verknüpfen (behavioral analysis). So kann es z.B. unkritisch sein, wenn auf sensible Daten zugegriffen wird. Geschieht dies allerdings nachts von einem unüblichen Standort aus, so kann dieses Zusammentreffen von Parametern zu einem gerechtfertigten Sicherheitsalarm führen. Diese erweiterte Auswertung fasst man unter dem Begriff »Korrelation von Sicherheitsereignissen« zusammen und wird in weitergehenden Ausbaustufen von SIEM-Umgebungen eingesetzt. Um dies erreichen zu können, ist es allerdings erforderlich, Daten aufzuzeichnen, die datenschutzrechtlich relevant sind. Um Muster verdächtiger Anmeldevorgänge zu erkennen, muss man zunächst wissen, wann sich welcher Benutzer von wo aus einloggt. Diese Daten zu erfassen, widerspricht zunächst dem Prinzip der Datensparsamkeit. Erst wenn eine unübliche, nächtliche Anmeldung erfolgt, ergibt sich in der Korrelation mit den Daten der normalen Anmeldezeiten und Orte der Zweck der Erfassung. Das Spannungsfeld ist vergleichbar mit der Diskussion um Big Data und sollte unter Einbezug aller Beteiligten im Vorfeld geführt werden.

11.3 Ebenen des Monitorings

Das Monitoring von IT-Systemen hat lange Zeit ein eher unscheinbares Dasein gefristet. Das änderte sich zusehends mit der wachsenden Diversifizierung der IT-Landschaft und der Abhängigkeit von Softwaresystemen. Laut Studien können die allermeisten großen Unternehmen Ausfälle von zentralen IT-Systemen über eine Dauer von zehn Arbeitstagen nicht mehr verkraften und geraten dann in eine kritische Situation. Es ist in diesen Fällen nicht nur wichtig, zu erfahren, dass etwas passiert ist, sondern vielmehr, wo es passiert ist. Natürlich ist der Mehrwert nur dann gegeben, wenn die Einführung eines Monitoring-Systems mit einer Strukturierung und Darstellung der aufeinander aufbauenden und damit voneinander abhängigen Systeme einhergeht.

Heutige IT-Landschaften sind zumeist hoch komplex. Das bezieht sich nicht nur auf einzelne Hosts und die darauf installierte Software, sondern vielmehr



auf die komplizierten und häufig wechselnden Beziehungen der IT-Systeme untereinander. Spätestens, wenn mehrere Hundert Hosts im Einsatz sind, wird es unerlässlich sein, diese zu gruppieren und die Abhängigkeiten untereinander zu visualisieren. Ist es für den Systemadministrator interessant, zu wissen, dass ein bestimmter Host ausgefallen ist, so kann es für die fachlich verantwortlichen Personen wichtiger sein, welche Services ihrer Abteilung dadurch nur eingeschränkt erbracht werden können. Das hat unter anderem mit den Service Level Agreements (SLA) zu tun, die gegenüber dem Kunden kommuniziert wurden. Auf der nächsthöheren Ebene wird selbst dies zu technisch und zu abstrakt sein. Dort wird die Frage gestellt, welche kritischen Business-Prozesse vom Systemversagen bedroht sein könnten.

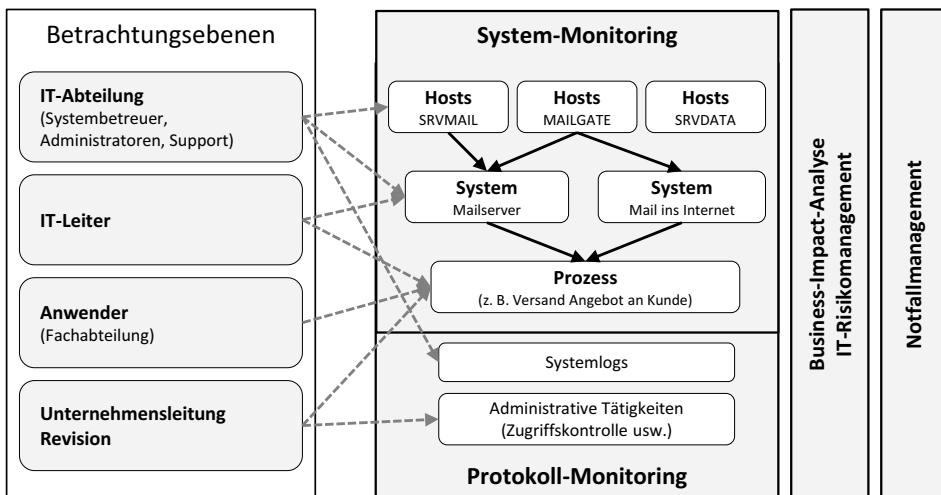


Abbildung 11.2: Monitoring betrachtet aus verschiedenen Perspektiven

In Abbildung 11.2 sind die verschiedenen Perspektiven abgebildet, aus denen der Blick auf Ereignisse stattfinden kann. Auch wenn es sich immer um dieselben Events handelt, ist das Interesse jeweils anders gelagert. Neben der IT-Security, die einen Blick auf sicherheitskritische Ereignisse hat, werden auch die IT-Abteilung und alle von der IT abhängigen Unternehmensbereiche Interesse an diesen Daten haben. Der Verdichtungsgrad ändert sich dabei von Ebene zu Ebene deutlich.



11.4 System-Monitoring

Vom Ansatz her ist der Betrieb eines System-Monitorings eine vergleichsweise unkomplizierte Sache. Schon ein periodisch durchgeföhrter Ping zu einem Webserver und die Auswertung der Antwort deckt bereits die Frage ab, ob der Server per Netzwerk erreichbar ist oder nicht. Eine Telnet-Verbindung auf den http-Port, also Port 80, und die Auswertung der Antwort liefert zudem die Information, ob der Webserver-Dienst Anfragen entgegennimmt. Zwei einfache, in den meisten Betriebssystemen mit Bordmitteln zu realisierende Maßnahmen und ein Webadministrator können bereits wichtige Aussagen über die allgemeine Verfügbarkeit eines IT-Systems und der darauf installierten Applikationen treffen.

11

Wo liegt also die Herausforderung? Die Herausforderung wächst mit der Komplexität der Umgebung und mit den Anforderungen der Administratoren und der verschiedenen Leitungsebenen. Zudem müssen auch die Zuverlässigkeit und die Verfügbarkeit eines Monitorings gewissen Standards genügen. Für einen Webserver können die oben aufgeführten Maßnahmen bereits ausreichend sein, für Hunderte von Servern wird die schiere Masse zum Problem. Dazu kommen die Zusatzfragen der Art: »Wie häufig ist er denn schon ausgefallen?« oder »Kann man den Speiseplan aufrufen, wenn WEBSRV01 nicht antwortet?« Die erste Frage deutet in die Richtung Datenbank und Aufzeichnung vergangener Ereignisse. Die zweite Frage deutet schon an, dass es Personen gibt, die nicht unbedingt an einem speziellen IT-System interessiert sind, sondern vielmehr an deren Services. Der Erfahrung nach wird dies umso ausgeprägter der Fall sein, je höher in der Unternehmenshierarchie eine Person angesiedelt ist. Ist der Administrator noch mit der Aussage zufrieden, dass Host SRVMAIL01 antwortet, so will der IT-Leiter nur noch wissen, ob der Versand von E-Mails noch funktioniert.

Monitoring aus Sicht eines IT-Security-Verantwortlichen bedeutet nicht nur die Erhöhung der Verfügbarkeit, wie im Kapitel »Business Continuity Management« beschrieben, sondern genauso die Schaffung von Transparenz durch alle Ebenen der IT-Infrastruktur. Das bezieht sich auf Systeme genauso wie auf Software, Betriebssysteme, Daten und den Netzverkehr. Transparenz bedeutet in diesem Fall schlicht die Erfassung und automatisierte Auswertung von Datenströmen. Dieser Vorgang wandelt reine Daten in Informationen um, indem Regeln angewendet und Daten miteinander verknüpft werden.



11.4.1 Sicherheitsaspekte

Die Überwachung von Hosts kann nur funktionieren, wenn dem überwachten System gewisse Rechte auf dem Zielsystem zugebilligt werden. Das kann vom Zugriff auf den SNMP-Provider bis hin zum Vollzugriff reichen. Der Zugriffslevel ist zum einen abhängig von der Art der überwachten Funktionen und zum anderen von den Anforderungen der Monitoring-Software. Werden Agenten auf dem Zielsystem direkt installiert, so werden diese zumeist in einem Kontext arbeiten, der weitreichende Rechte auf die Systemressourcen hat.

Die Beschränkung der Rechte auf das absolut erforderliche Maß ist eine Vorgehensweise, die auch beim Einsatz von Monitoring verfolgt werden muss. Dazu gehören die Beschränkung von SNMP auf den Lesemodus, die Verschlüsselung des Netzwerkverkehrs zwischen Monitoring-System und Zielrechner und die Beschränkung abgefragter Ports auf das Nötigste. Auch muss bedacht werden, dass die Sammlung von Systemevents und Sicherheitsevents zu einer Datenbasis an sicherheitsrelevanten Informationen führt. Diese Datenbasis kann wiederum missbraucht werden, um gezielte Angriffe zu fahren oder aber durch Analyse der Daten herauszufinden, welche Art von Angriff durch das System nicht erkannt wird. Finden sich z.B. in der Datenbank keine Einträge über gesperrte Benutzerkonten aufgrund zu vieler fehlerhafter Passworteingaben, so weiß der Angreifer, dass solcherart Angriffe nicht durch dieses System erfasst werden.

11.4.2 Auswahl zu überwachender Systeme

Monitoring-Systeme sind unentbehrlich, wenn es darum geht, den Zustand der IT-Dienstleistungen zu jedem Zeitpunkt zu bewerten und um schnell und zielgenau auf Störungen zu reagieren. Gut implementiert liefern sie die Meldungen, die man benötigt, an genau die Personen, die für die Problemlösung verantwortlich sind. Meldungen darüber, dass die Kapazität von Plattsystemen bei < 10 % angelangt ist, obwohl dies den Normalzustand darstellt, können das gesamte System sehr schnell in die Knie zwingen und den Administrator des Monitoring-Systems überfordern. Der Spagat zwischen zu vielen Meldungen und der Nichtbeachtung einer Störung, die später zu einem Notfall wird, ist nicht einfach zu bewältigen.



Werden alle vorhandenen Hosts unreflektiert mit in das Monitoring integriert, so ist nicht nur der anfängliche Aufwand erheblich, es schlägt sich auch auf den laufenden Betrieb nieder. Wichtiger Bestandteil eines Monitoring-Projekts wird es also immer sein, basierend auf der Business-Impact-Analyse die Priorität der Business-Prozesse, die dazugehörigen IT-Services und schlussendlich die IT-Systeme zu definieren, die zu überwachen sind. Diese Feststellung ist nicht nur für Großunternehmen gültig. In kleineren Betrieben wird es zwar weniger Systeme geben, und vermutlich werden auch die Verknüpfungen untereinander weniger komplex sein, auf der anderen Seite stehen aber auch in den meisten Fällen weniger Ressourcen und weniger Budget für eine Softwarelösung und deren Pflege zur Verfügung.

11.4.3 Implementierung im Netzwerk

11

Vom Konzept her bedeutet Monitoring, dass Applikationen auf IT-Systemen Attribute der eigenen Umgebung oder anderer IT-Systeme abfragen und speichern. Abhängig von der Aufgabenstellung kann es eine ganze Bandbreite unterschiedlicher Systembereiche geben, die überwacht werden müssen. Eine der einfacheren IT-Funktionen, die überwacht werden kann, ist die Konnektivität im Netzwerk. Durch periodisch durchgeführte Netzwerkkabfragen kann überprüft werden, ob das Zielsystem noch im Netzwerk erreichbar ist. Bricht die Verbindung ab, so kann dieses Ereignis durch Alarmanzeigen, SMS-Mitteilungen oder z.B. durch Versand einer E-Mail an den Administrator eskaliert werden. Schwieriger wird es, wenn es darum geht, die Funktionalität einer Anwendung auf einem IT-System zu überprüfen. In diesem Fall gibt es klassischerweise zwei Möglichkeiten. Zum einen können Logfiles der Anwendung regelmäßig durch das Monitoring-System ausgelesen und interpretiert werden, und zum anderen kann vom Monitoring-System aus überprüft werden, ob die Anwendung auf dem Zielsystem auf Anfragen korrekt antwortet. Ein Beispiel wäre das Monitoring eines Mailsystems. Die Überprüfung der Funktionalität könnte in diesem Fall so aussehen, dass eine E-Mail versandt wird und deren Eingang automatisiert bestätigt, dass der Service »E-Mail-Versand« korrekt funktioniert.

Abhängig von der Anzahl an zu überwachenden Zielsystemen und von der Netzwerkinfrastruktur kann es schon aufgrund von Laufzeitproblemen zu Fehlmeldungen kommen. Antwortet ein überwachter Host deshalb nicht rechtzeitig, weil die Verzögerungen durch eine langsame WAN-Anbindung



zu groß werden, so kann es zu Falschmeldungen (*false positives*) kommen. Dasselbe kann auch schon dann passieren, wenn der Monitoring-Server überlastet ist. Daraus kann man ableiten, dass der Standort des Überwachungsservers und die Beschaffenheit der Netzwerkinfrastruktur genauso zu beachten sind wie die Hardwareausstattung aller beteiligten Komponenten. Grundsätzlich gilt, dass überwachte Systeme möglichst im gleichen Netzwerk wie die Monitoring-Server implementiert werden sollten. Je weniger Fernverkehrsnetze, Router, Switches oder Firewalls zwischen den Geräten stehen, desto besser.

Bei der Überwachung eines Hosts, der hinter einer Firewall installiert ist, kommen weitere Hindernisse hinzu. So kann es für den Abteilungsleiter wichtig sein, den Backupdienst überwacht zu wissen, aber der Systemadministrator der Firewall wird ungern alle dafür erforderlichen Ports zum internen Netz öffnen, nur um das Monitoring zu ermöglichen. Interessenkonflikte wie dieser können häufig durch sogenannte »Monitoring-Agenten« gelöst werden. In diesem Beispiel würde ein solcher in der DMZ des Zielsystems implementiert werden. Damit wäre es nur noch nötig, einen Port zwischen dem Agenten und dem zentralen Monitoring-System zu öffnen. Jeder weitere Traffic bezüglich des Monitorings würde nur noch zwischen dem Agenten und dem Zielsystem stattfinden.

11.5 Protokoll-Monitoring

Im Gegensatz zum System-Monitoring überwacht und wertet man beim Protokoll-Monitoring, auch als Logfile-Monitoring bezeichnet, Protokolldateien aus, die von Betriebssystemen oder Anwendungen geschrieben werden. Es sind vorwiegend zwei Vorteile, die eine konsolidierte Überwachung von einer zentralen Stelle aus bieten. Zum einen wird es dadurch möglich, Zusammenhänge zu visualisieren, also sicherheitsrelevante Vorfälle aufzudecken, die nur dann sichtbar werden, wenn mehrere Protokolle verschiedener IT-Systeme in einen Zusammenhang gebracht, also korreliert werden. Zum anderen können nachträglich Sicherheitseignisse recherchiert werden. Ein Beispiel für die nachträgliche Ermittlung in einem Sicherheitsvorfall unter Hinzunahme der Korrelierung der Daten ist ein Fall, in dem Daten von einem Windows-Server gestohlen wurden. Die Ermittlung, welche Daten entwendet wurden und von welchem Rechner aus der Zugriff geschah, erfolgt durch Analyse des Event-Logs. Die Datenbank des DHCP-Servers, also der Instanz,



die die IP-Adresse vergibt und damit den Zugang zum Netzwerk ermöglicht, gibt die MAC-Adresse des Angreifers heraus und die Durchsicht der Router- und Switchprotokolle letzten Endes den genauen Netzwerkport und damit die Lokation, von der aus der Angreifer gearbeitet hat. Auf diese Weise werden Einträge aus drei verschiedenen Log-Dateien genutzt, um den Angriffspfad möglichst detailliert nachzubilden zu können.

Hinweis

Der Begriff »Logfiles« darf nicht allzu wörtlich genommen werden. Natürlich kann es sich auch um Textdateien im Dateisystem handeln, aber genauso können Datenbankeinträge abgefragt werden oder Systeme und Applikationen senden Informationen direkt über definierte Schnittstellen an das erfassende System. Das nennt man dann »Syslog«. Bei Syslog handelt es sich um ein Netzwerkprotokoll, das speziell für die Übertragung von Logfiles genutzt wird.

11

Daten zu erfassen, um sie zu einem späteren Zeitpunkt auswerten zu können, führt automatisch dazu, dass man so viele Daten wie möglich erfasst, da man nicht weiß, welche Daten genau wichtig sein werden. Die Umgebung, in der dies geschieht, ist das bereits erwähnte SIEM. Ein SIEM ist damit im Grunde eine große Datensammlung mit häufig mehreren Gigabytes täglich hinzukommender Daten, die zentral gespeichert wird. Über Index-Mechanismen und schnelle Algorithmen ist es dennoch möglich, in wenigen Sekunden Terabyte an Daten strukturiert zu durchsuchen. Die Darstellung wird üblicherweise in Listen und Dashboards angeboten mit der Möglichkeit, Berichte zu erstellen. Diese Darstellung ist dann sowohl für den Leiter der IT als auch für den Administrator nützlich, der die Aufgabe hat, Sicherheitsrisiken zu reduzieren.

11.5.1 Unterstützung von Audits

Durch die Möglichkeit, das Protokoll-Monitoring weitgehend zu automatisieren, dient sie der täglichen Kontrolle von sicherheitsrelevanten Problemen wie: »Hat sich heute jemand fünfmal mit falschem Passwort angemeldet?« oder »Gab es Zugriffe auf sensible Daten außerhalb der normalen Arbeitszei-



ten?« Ereignisse dieser Art können genauso wie beim System-Monitoring in Echtzeit gemeldet werden. Die weitere Recherche kann dann mit vorgefertigten Abfragen vertieft werden.

Neben der Möglichkeit des Echtzeit-Monitorings kann das Protokoll-Monitoring zur Unterstützung von Audits herangezogen werden. Audits (also Kontrollen, ob der Ist-Zustand dem Soll-Zustand entspricht) werden zumindest zum Teil auch darauf basieren, dass über die Auswertung von Protokollen auf die Umsetzungsqualität von Maßnahmen geschlossen wird. So kann die Frage, ob sich Administratoren wirklich nicht mit ihrem administrativen Benutzer für ihr Tagesgeschäft am lokalen Arbeitsplatzrechner anmelden, dadurch geklärt werden, dass die Protokolle erfolgreicher Anmeldungen auf genau diesen Sachverhalt untersucht werden.

11.5.2 Überwachung administrativer Tätigkeiten

Ein heikler Punkt, der spätestens dann auftaucht, wenn von einer Umsetzung von EU-DSGVO-Vorgaben die Rede ist, beinhaltet die Überwachung administrativer Tätigkeiten. Also die Aufzeichnung und Auswertung von »Was hat welcher Administrator zu welcher Zeit getan?« Dass eine Implementierung eines solchen Systems der Abstimmung mit dem Betriebsrat bedarf, ist selbstverständlich und auch, dass mit den Administratoren darüber gesprochen werden muss. Aber auch die Auswahl eines Verfahrens und letztendlich eines Tools muss wohlüberlegt sein. Eine Auswertung dieser Art dient häufig nicht der Fehlersuche, sondern kann bei gewissen Ergebnissen durchaus zu personalrechtlichen Konsequenzen führen. Nicht zuletzt deshalb ist sicherzustellen, dass die Protokolldaten und die Daten in der Datenbank des Tools nicht manipuliert werden können und dass der Zugriff idealerweise im Vier-Augenprinzip stattfindet.

Auf der anderen Seite werden Daten heute auf der einen Seite klassifiziert und auf der anderen Seite können Administratoren darauf zugreifen, auch wenn sie aufgrund ihrer Einstufung nicht dazu in der Lage sein sollten. Mit der Einführung eines IT-Risikomanagements erfolgt deshalb auch immer häufiger ein Umdenken. Weg von dem starren System »Wir vertrauen unseren Administratoren grundsätzlich« hin zu einem weit differenzierteren Bild. In dieses neu entstehende Bild passen Werkzeuge zur Protokollüberwachung hinein.



11.5.3 Schwachstellenmanagement

Eine wichtige Anforderung an die Transparenz ist es, die Schwachstellen von eingesetzten Betriebssystemen, Firmware, Hardware oder Applikationen zu kennen. Nur wenn sicherheitsrelevante Schwachstellen im Chip-Design oder Software-Code bekannt sind, können Gegenmaßnahmen wie das Patchen eingeleitet werden. Die Systeme, die genutzt werden, um gezielt nach Schwachstellen zu suchen, werden »Schwachstellen-Scanner« genannt und funktionieren üblicherweise auf zwei grundlegend unterschiedliche Arten: Sie scannen entweder passiv den Netzwerkverkehr und ziehen daraus Schlüsse oder sie kommunizieren direkt mit offenen Netzwerk-Ports von IT-Systemen und versuchen über diesen Weg, Release-Stände von Software zu ermitteln, oder führen direkt eingeschränkte Penetrationstests durch.

11

Passiver Scan des Netzwerkverkehrs

Vorwiegend in Bereichen, in denen fragile IT-Systeme im Einsatz sind, wird auf die passive Überwachung des Netzwerkverkehrs gesetzt. Dabei kann es sich z.B. um stark inhomogene Produktionsumgebungen handeln. Zum Einsatz kommen dabei Sensoren, die z.B. an den Spiegel-Ports von aktiven Netzwerkkomponenten angeschlossen werden. Aus dem mitgelesenen Netzwerkverkehr lassen sich dann Rückschlüsse auf die Kommunikationsbeziehungen zwischen den Geräten, auf deren Eigenschaften und auf die Eigenschaften und Versionen von Software ableiten.

Direkte Scans von IT-Systemen

Services oder Applikationen auf IT-Systemen kommunizieren über geöffnete Ports. Sendet man z.B. eine entsprechende Anfrage an einen Webserver auf Port 80 (unverschlüsselt) oder 443 (verschlüsselt), erhält man sowohl Informationen über den Inhalt von Webseiten als auch über die eingesetzte Webserver-Software. Stellt man dabei z.B. fest, dass eine veraltete Software eingesetzt wird, für die nicht nur Schwachstellen, sondern auch Exploits, die diese ausnutzen können, existieren, muss ein Administrator entsprechende Maßnahmen einleiten. Schwachstellenscanner können aber noch einen Schritt weiter gehen und einfache, automatisierte Angriffe gegen solche Systeme durchführen. In diesem Beispiel wären Ziele eines solchen Angriffs z.B. das Herauslesen von Passwörtern oder der Zugriff auf Datenbanken, auf die der Webserver zugreift.



Der Begriff »Schwachstellenmanagement« beschreibt den gesamten Prozess von der Implementierung von Scannern über das Scannen selbst bis hin zur Identifikation und Nachverfolgung von Schwachstellen. Innerhalb einer SIEM-Lösung können die Ergebnisse im Rahmen von Dashboards und Listen visualisiert und den verschiedenen Interessengruppen zugänglich gemacht werden.





12 IT-Security-Audit

12.1 Kapitelzusammenfassung

Das Ziel eines transparenten und nachprüfbareren Sicherheitsniveaus macht die Durchführung von Audits erforderlich. Keine Richtlinie ohne Prüfung der darin enthaltenen Vorgaben! Das muss eine klare Aufgabenstellung der IT-Security-Organisation darstellen. Damit bilden IT-Security-Audits das Bindeglied zwischen Vorschriften in Form von Richtlinien und der tatsächlich gelebten Wirklichkeit.

12

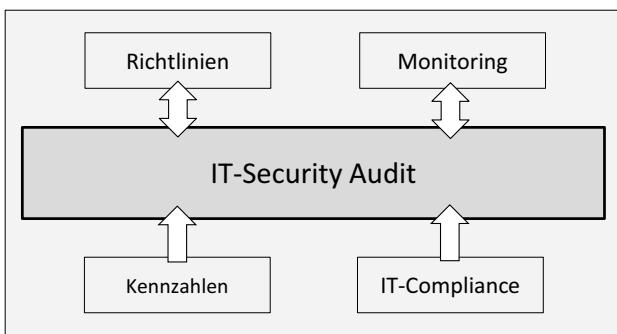


Abbildung 12.1: Primäre Abhängigkeiten von anderen Themen der IT-Security

Das aktuelle Kapitel zeigt auf, wie Audits innerhalb eines Unternehmens platziert werden sollten und wie eine Durchführung in der Praxis aussehen könnte.

Die Top-4-Fragen zum aktuellen Kapitel:

- Ist eine IT-Security-Audit-Organisation installiert und mit ausreichend Ressourcen ausgestattet?
- Wird die Umsetzung von Vorgaben aus Richtlinien regelmäßig überprüft?
- Werden die Ergebnisse aus Audits strukturiert aufbereitet und wird damit eine Vergleichbarkeit von Prüfung zu Prüfung sichergestellt?
- Ist sichergestellt, dass eine objektive Bewertung während eines Audits stattfinden kann?



12.2 Einführung

In einem Unternehmen steht eine ganze Reihe an Bereichen im Fokus von internen Audits. Diese Audits werden üblicherweise durch eine zentrale Organisation, die interne Revisionsabteilung, durchgeführt, die zu diesem Zweck unabhängig sein muss und deshalb häufig an der Unternehmensleitung aufgehängt ist. Die Revisionsabteilung wird in den meisten Fällen auch die IT-Abteilung prüfen und dabei auch Punkte der IT-Security zumindest streifen. In das Detail zu gehen, ist allerdings häufig nicht der Fall und an dieser Stelle wird dann die eigene IT-Security-Audit-Organisation aktiv. Diese ist dann meistens in der IT-Abteilung aufgehängt.

Ein Informationsaustausch und die Abstimmung von Audits mit der Revisionsabteilung sind wichtig und helfen der IT-Security-Audit-Organisation, trotz des Interessenkonflikts, bei Installation in der IT einen gewissen Grad an Objektivität zu bewahren. Idealerweise ist auch die IT-Security-Audit-Organisation unabhängig von der IT aufgestellt und mit eigenen Experten besetzt. Die Trennung von der IT bringt allerdings wieder Nachteile mit sich, wenn es um technische Details in der Prüfung geht, die sozusagen von Kollege zu Kollege leichter zu erfassen und zu bewerten sind.

Unter dem Begriff »IT-Security-Audit« kann man alle Vorgänge zusammenfassen, die sich damit beschäftigen, den Status des Sicherheitsniveaus zu erfassen und zu bewerten. Ein Audit kann damit maschinell stattfinden, durch technische automatisierte Überprüfung vorgegebener Kennzahlen oder auch manuell z.B. in Vieraugengesprächen mit Administratoren. In allen Fällen werden die Ergebnisse in einer möglichst vorgegebenen Form niedergeschrieben und anschließend bewertet. Abhängig von den Ergebnissen werden dann entsprechende Maßnahmen abgeleitet und nachverfolgt.

12.3 Audits im Kontext des IT-Security-Managements

Die Aufgabe des IT-Security-Managements ist es, Risiken für das Unternehmen zu erkennen, diese zu bewerten und Maßnahmen dagegen zu ergreifen. Die Durchsetzung von Maßnahmen wird durch die Erstellung von Richtlinien flankiert. Der Grad der Umsetzung von so definierten Maßnahmen und den in Richtlinien festgelegten Vorgaben wiederum wird im Rahmen der



Durchführung von Audits festgestellt. Audits stellen damit einen wichtigen Teil des Kontrollmechanismus des IT-Security-Management-Zyklus dar und sind wesentlich dafür verantwortlich, Schwachstellen und Versäumnisse zu erkennen, auf die Umsetzung von bereits definierten Maßnahmen zu drängen oder aber eine Neubewertung anzustoßen.

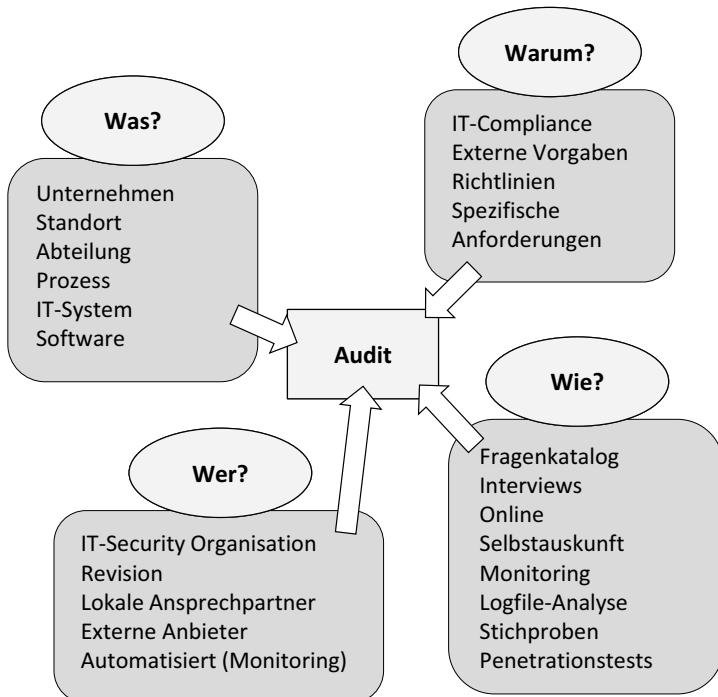


Abbildung 12.2: Vier Perspektiven auf IT-Security-Audits

Die Überprüfung, inwieweit Vorgaben auch eingehalten werden, ist eine maßgebliche Funktion der IT-Security-Organisation. Regeln ohne eine nachträgliche Überprüfung aufzustellen, führt nicht nur zu einem unkalkulierbaren Sicherheitsniveau, sondern blockiert zudem auch die Weiterentwicklung.

Der Regelkreis der kontinuierlichen Verbesserungen basiert zu einem nicht unwesentlichen Teil auf den Rückmeldungen, die aus Sicherheits-Audits heraus entstehen. Davon, dass ein Audit durchgeführt wird, von dessen Qualität und der Art des Audits hängen die Qualität der Rückmeldungen, die daraus generierten Maßnahmen und damit das Sicherheitsniveau als Ganzes ab.



KAPITEL 12 – IT-SECURITY-AUDIT

Neben den eigenen Richtlinien wird ein Audit gewährleisten müssen, dass ein objektiver Blick auf den Umsetzungsgrad gesetzlicher und anderer Vorgaben eingehalten wird.

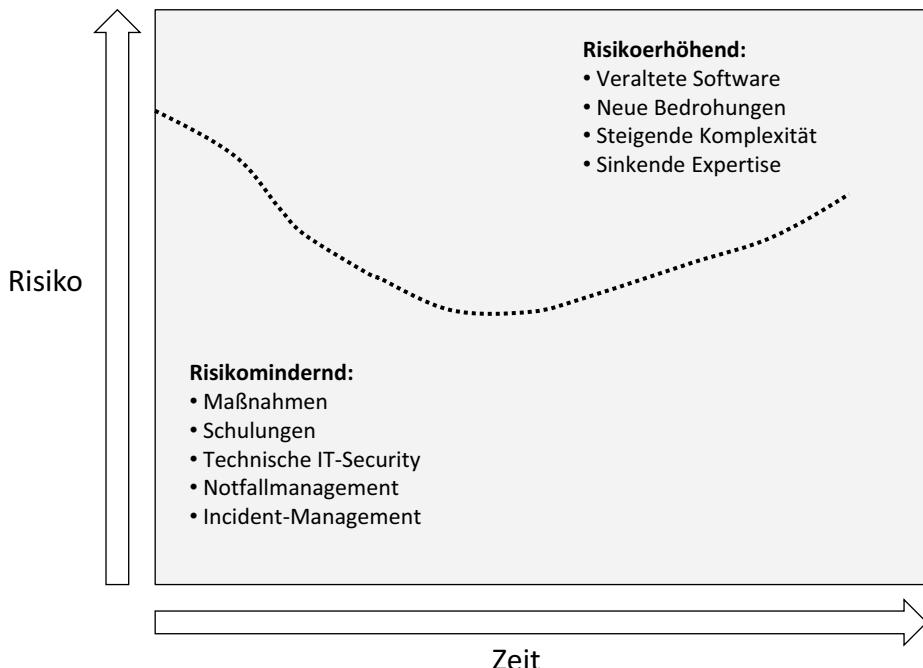


Abbildung 12.3: Veränderung eines Risikos über die Zeit

Das Niveau von Bedrohungen, Eintrittswahrscheinlichkeiten und auch die Klassifikation eines Wertes sind über die gesamte Lebenszeit betrachtet nicht statisch. Viele Faktoren mindern oder erhöhen das Risiko für einen Wert und damit indirekt für das Unternehmen. Regelmäßige Audits ermöglichen es, den Ist-Zustand zu einem definierten Zeitpunkt zu erfassen, zu bewerten und mit den Ergebnissen vorausgegangener Audits zu vergleichen. Aus diesen Ergebnissen können dann in einem zweiten Schritt die erforderlichen weiteren Schritte wie ein IT-Risikomanagement und die Umsetzung daraus resultierender Maßnahmen abgeleitet werden.

Ein Audit liefert damit Informationen, die Transparenz schaffen, und deckt auch Risiken auf, die es entweder zuvor noch nicht gegeben hat oder aber die bei bestehenden Prozessen aufgrund externer Einflüsse größer geworden sind.



Tipp

Werden Audits standardisiert, dann liefern sie Ergebnisse, die den Vergleich von Standorten oder auch die Entwicklung über die Zeit ermöglichen. Diese Ergebnisse visualisieren die Entwicklung des Sicherheitsniveaus.

In Abbildung 12.4 ist zu erkennen, wie sich das Sicherheitsniveau in verschiedenen Standorten eines Unternehmens in den Jahren 2009 bis 2011 entwickelt hat. Eine Übersicht dieser Art wird auch als IT-Security-Landschaft (IT-Security Landscape) bezeichnet und visualisiert auf einen Blick nicht nur die Entwicklung, sondern ermöglicht es auch, durch den Vergleich mehrerer Standorte Rückschlüsse zu ziehen.

12

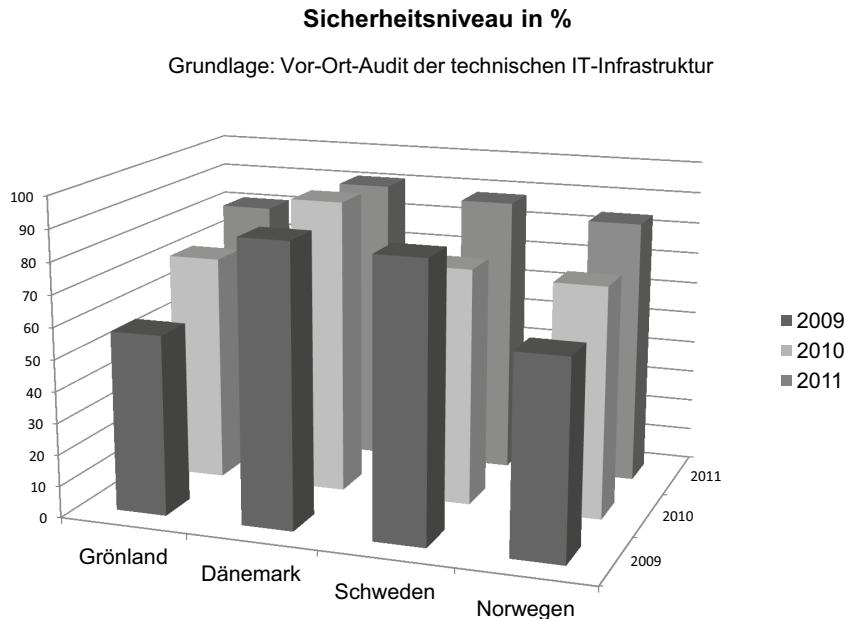


Abbildung 12.4: Darstellung des Sicherheitsniveaus

Ein Manager IT-Security verantwortet Maßnahmen und damit Investitionen. Diese müssen auf einer Grundlage getätigt werden, die verlässlich und nach-



vollziehbar dargestellt werden kann. Einen Teil dieser Grundlage kann ein Audit liefern. Das Audit zeigt das Delta auf zwischen Erwartung und Ist-Zustand oder die Entwicklung zwischen Standort A und Standort B zum Zeitpunkt T. Damit gehört es zusammen mit dem IT-Risikomanagement zu den wesentlichen Instrumenten bei der Argumentation, an welcher Stelle welche Maßnahmen zu installieren sind. Die Grundlage muss dafür aus der IT-Strategie ableitbar sein, und zwar der Wille der Unternehmensführung, ein gleiches und sinnvolles Sicherheitsniveau über das gesamte Unternehmen zu etablieren. Das Audit dient zur Überprüfung, ob dieses Ziel erreicht wird, aber auch der Feststellung, wie weit man davon noch entfernt ist. Es ist also ein regulierendes Instrument, das auf verschiedenen organisatorischen Ebenen eingesetzt werden kann.

12

12.4 Audits im Unternehmenskontext

Nach einer Festlegung der grundlegenden Audit-Organisation und der Schnittstellen zu anderen Sicherheitsbereichen, der Revision und dem Datenschutzbeauftragten hat die Unternehmensleitung die weitergehende Aufgabe, Audit-Strategien einzufordern und einen kontinuierlichen Prozess im Unternehmen zu etablieren.

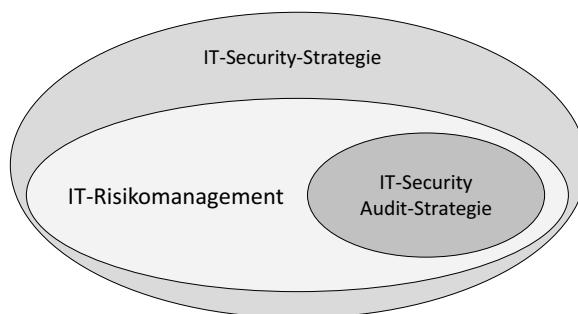


Abbildung 12.5: Einordnung der Audit-Strategie

Die Langfristplanung von Audit-Prozessen folgt der Unternehmensstrategie im weiteren Sinne und steht im direkten Zusammenhang mit der IT-Strategie. Sieht die Unternehmensstrategie eine Neuausrichtung hin zu einer neuen Produktsparte vor oder gewinnt eine Produktsparte an Bedeutung, dann wird dieser Ausrichtung auch die IT-Strategie folgen und dementsprechend auch die Schwerpunkte der Audit-Organisation. Das kann sich auf eine



sich verschiebende Priorisierung von bestimmten Daten, IT-Systemen oder Standorten auswirken.

12.5 Audits nach Kategorien

Ein Audit vor Ort über mehrere Tage, unter Umständen in einem anderen Land, bindet in hohem Maße Kapazitäten. Nicht nur die des Auditors und seines Teams, sondern auch die der Experten vor Ort, die befragt werden müssen. Technische Auswertungen erfordern mit hoher Wahrscheinlichkeit die Anwesenheit eines Administrators oder eines Softwareentwicklers. Dazu kommt die Nacharbeit in Form der Auswertung und der Erstellung des Berichts. Man kann schnell erkennen, warum das Mittel des Audits nur sparsam eingesetzt wird, und in größeren Unternehmen mit vielen Standorten führt dies sehr schnell dazu, dass umfassende Vor-Ort-Audits nur alle paar Jahre durchgeführt werden. In der Zwischenzeit werden häufig zielgerichtete Audits angesetzt, die sich nur auf Teilgebiete konzentrieren.

Jede Phase einer Softwareentwicklung, des Betriebs von IT-Systemen oder dem Ablauf von Prozessen kann durch ein Audit gezielt überprüft werden. Dementsprechend kann man hier unter vielen anderen von Evaluierungs-, Vor-, Implementierungs-, Betriebs-, Prozess-, Gebäude- oder System-Audits sprechen.

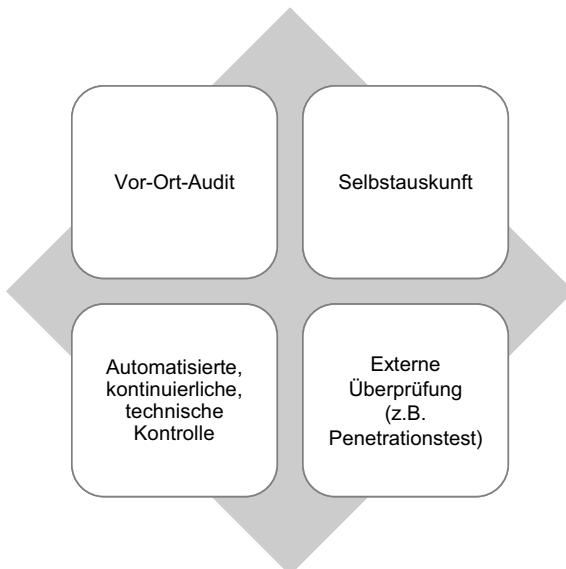


Abbildung 12.6: Kategorien von Audits



Hinzu kommt, dass es durchaus üblich ist, bestimmte Formen des Audits für definierte Bereiche eines Unternehmens individuell zu gestalten. So kann es sinnvoll sein, Prozess-Audits in der Personalabteilung anders zu gestalten als im Entwicklungsbereich.

Hinweis

Um das Werkzeug Audit zielgenau einsetzen zu können, findet das umfassende Audit mit Hunderten von Fragen heute kaum noch Verwendung. Dieses wird ersetzt durch eine ganze Reihe von Audit-Kategorien, die sich auf Teilbereiche konzentrieren und zudem abteilungsspezifisch eingesetzt werden können. Ziel dieser Diversifizierung ist es, Audits modularer anzulegen und bei Bedarf individuelle Audits erzeugen zu können. Diese Vorgehensweise soll trotzdem eine weitgehende Standardisierung ermöglichen.

12

Audits, die auf Fragebögen basieren, die individuell für einen Standort, eine Abteilung, einen Bereich, ein IT-System oder eine Software zusammengestellt wurden, haben gemeinsam, dass sie mit einem Vorlauf angekündigt werden und dann gezielt an einem bestimmten Termin stattfinden. Änderungen an der Sicherheitslage zwischen Abschluss des Audits und einer Nachauditierung oder einem neu angesetzten Audit werden nicht registriert. Um diese Zeiträume zu überbrücken, werden üblicherweise Methoden angewendet, die eine kontinuierliche Überprüfung ermöglichen. Zu diesen Methoden gehört der Einsatz von Tools, die eine Auswertung von Protokollen von IT-Systemen erlauben, das Monitoring oder aber die Nutzung von automatisierten Penetrationstools. Alle diese Informationen werden wiederum in einem SIEM verarbeitet und dargestellt. Auch externe Dienstleister bieten vermehrt an, interne IT-Systeme und IT-Systeme, die vom Internet aus erreichbar sind, auf regelmäßiger Basis einem Penetrationstest zu unterziehen. Es muss dem Manager IT-Security aber immer bewusst sein, dass ein automatisierter Penetrationstest oder die fallweise Überprüfung von Protokolldateien ein persönlich durchgeführtes Vor-Ort-Audit nicht ersetzen kann.



12.6 Vor-Ort kontra Selbstauskunft

Die Wörter »Audit« und »Auditor« können vom lateinischen Wort »audire« für zuhören abgeleitet werden. Das legt bereits nahe, dass ein Audit vor allem durch eine Befragung von Personen, die Durchführung von Stichproben, eine persönliche Auswertung von Protokolldateien und technische Tests gekennzeichnet ist. Sowohl bei einem Audit, bei dem der Auditor vor Ort erscheint, als auch bei einer Selbstauskunft (*self assessment*), bei der ein Fragebogen verschickt wird, ist die Interaktion zwischen dem Auditor und dem lokalen Experten erforderlich.

In einer IT-Security-Organisation, die in jedem Standort einen (Teilzeit-)Verantwortlichen für IT-Security einsetzt, wird der Fragebogen zur Selbstauskunft von dieser Person ausgefüllt. In Unternehmen, in denen keine solche Person zur Verfügung steht, falls z.B. der Standort zu klein ist, ist es wichtig, dafür zu sorgen, dass die Überschneidung von Tagesaufgaben und Audit-Bereich so weit wie möglich minimiert ist. Es ist nicht sinnvoll und oft auch nicht aussagekräftig, wenn der Administrator eines Systems selbst die Qualität seiner Arbeit beurteilen soll.

Ein bewährter Ansatz ist der, eine Selbstauskunft durch eine Person außerhalb der IT-Abteilung leiten zu lassen. Häufig wird dafür ein Mitarbeiter der Personalabteilung oder des lokalen Controllings herangezogen. Der Fragenkatalog sollte, alleine schon, um Fehlauskünfte zu vermeiden, so klar und einfach gestaltet sein, dass auch mittleres Wissen um die IT und die IT-Security ausreichen sollte, die Fragen zu bewältigen. Interviews mit Administratoren und Prozessverantwortlichen erleichtern zudem die Beantwortung der Fragen.

Trotz aller Vorkehrungen ist es offensichtlich, dass eine Selbstauskunft ein Vor-Ort-Audit nicht vollständig ersetzen kann. Hundertprozentige Neutralität ist nicht erzwingbar, und damit wird eine Selbstauskunft immer subjektiver ausfallen, als wenn die Bearbeitung durch einen Auditor von außerhalb stattfindet. Dazu kommt, dass das Niveau eines Berichts, der durch einen geschulten, neutralen Auditor erstellt wurde, einen deutlich höheren Grad an Vergleichbarkeit zwischen Standorten erlaubt. Auf der anderen Seite können regelmäßige Selbstauskünfte lange Perioden überbrücken, in denen kein Vor-Ort-Audit stattfindet. Das Zusammenspiel beider Spielarten ist aus diesem Grund in den meisten Unternehmen an der Tagesordnung.



12.7 Anforderungen an den Auditor

Eine Voraussetzung für ein glaubhaftes Audit ist die Sicherstellung der weitestmöglichen Unabhängigkeit des Auditors von den Bereichen, die er prüfen muss. Ein Auditor sollte niemals die eigene Arbeit oder die Arbeit der Organisationseinheit, in der er arbeitet, prüfen. Die Forderung nach der vorhandenen tief greifenden Expertise, die ein Auditor vorweisen muss, beißt sich in den meisten mittelständischen Unternehmen mit der ersten Anforderung. Hier ist der Auditor zumeist dieselbe Person, die die Regeln aufgestellt hat und die zudem verstrickt ist in Administration und Planung von sicherheitsrelevanten IT-Systemen. Einen vernünftigen Ausgleich zwischen den verschiedenen Anforderungen zu finden, ist Aufgabe der Unternehmensleitung.

12

Ein Audit im Rahmen des IT-Security-Managements stellt sich als geplante Befragung dar mit dem Zweck, den Ist-Zustand zu erfassen und gegen einen Soll-Zustand zu prüfen. Im Fokus liegen IT-Systeme und IT-Prozesse und die dadurch verarbeiteten Daten. Die Priorisierung der geprüften Systeme richtet sich nach den Erkenntnissen aus dem IT-Risikomanagement. Der Audit-Prozess beschäftigt sich mit allen Arbeitsvorgängen von der Organisation des IT-Audits über die Verankerung im Unternehmen bis hin zum Audit selbst sowie die Auffassung und Kommunikation eines Abschlussberichts, der erforderliche Maßnahmen genauso enthält wie eine Einschätzung des Deltas zwischen Erwartung und Ist-Zustand.

Der Auditor ist verantwortlich für die Vorbereitung, Durchführung und Nachbearbeitung eines Audits. Die verschiedenen Arten von Systemen, die auditiert werden können, erfordern Expertise in mehreren Fachbereichen. Ein Auditor, der die Sicherheit einer integrierten Software überprüfen soll, muss sich auf Expertenlevel mit dieser Software auskennen. Sollen zudem die IT-Systeme, auf denen die Software implementiert wurde, in ein Audit eingebunden werden, so wird weiteres spezifisches Wissen um Hardware, Netzwerke und Betriebssysteme erforderlich sein.

Es ist offensichtlich, dass es vielen Unternehmen nicht möglich ist, für jede dieser Fachbereiche einen spezialisierten Auditor zur Verfügung zu stellen. Aus diesem Grund wird ein Audit häufig von externen Spezialisten begleitet oder komplett durch sie durchgeführt. Eine Alternative besteht in der weitgehenden Einbindung der eigenen Administratoren.



Viele Unternehmen entscheiden nach einer Abwägung von Chancen und Risiken, was die Trennung von Funktionen, die Kosten für externes Consulting und die Ausbildung von Auditoren betrifft, die mit den Systemen betreuten IT-Mitarbeiter in das Audit mit einzubinden. Damit sparen diese Unternehmen Geld und setzen darauf, dass ein geschickter Auditor es dennoch schafft, ein möglichst hohes Niveau an Objektivität und damit für das Audit-Ergebnis ein hohes Niveau zu erhalten.

Damit zeichnet sich schon der Kreis der Teilnehmer ab. Dazu gehören, je nach Unternehmen in verschiedener Zusammensetzung, die folgenden Rollen:

- der leitende Auditor
- ein lokaler Auditor, häufig der Verantwortliche für IT-Security für den geprüften Bereich
- der IT-Leiter
- die IT-Spezialisten
- externe Berater
- die Unternehmensleitung, der die Ergebnisse präsentiert werden und die vorab die Aufgabe hat, die Ziele und die Erwartungen an das Audit zu formulieren
- Mitarbeiter der Revision, die unter Umständen bereits Teilebereiche durch ihre Prüfungen abdecken
- der Betriebsrat, falls es sich um Themen handelt, die deren Mitbestimmungsrechte berühren (Auswertung von Protokolldateien und Ähnliches)
- Mitarbeiter der Personalabteilung, wenn Verpflichtungen aus dem Arbeitsvertrag oder anderen Vereinbarungen wie die Geheimhaltung von Daten Thema eines Audits sind

Wie bereits erwähnt, sind die Anforderungen an die Qualifizierung eines Auditors abhängig von der Natur des untersuchten Objekts. Aus typischen Audits lassen sich damit Qualifikationsprofile ableiten wie:

- Auditor für Arbeitsplatzrechner
- Auditor für Server
- Auditor für die Datenspeicherung (Datenserver, Plattensysteme, Datensicherung und Datenwiederherstellung)



KAPITEL 12 – IT-SECURITY-AUDIT

- Auditor für einzelne Softwareprodukte
- Auditor für Produktsicherheit (z.B. Kundenprodukte, Prototypen, Steuersoftware etc.)
- Auditor für Netzwerke und Wireless-Umgebungen
- Auditor für Prozesse und Datenflussanalysen
- Auditor für physische Sicherheit (Rechenzentrum, Schließsysteme, Brandschutz, Wasser, Alarmierungssysteme, Werkschutz)

Alle Einzelqualifikationen enthalten jeweils auch Anforderungen für übergeordnete Aufgaben wie die Überprüfung des IT-Risikomanagements oder die Überprüfung des IT-Notfallmanagements für die einzelnen Felder.

12

12.8 Ein Audit Schritt für Schritt

Die Methodik, nach der ein Audit durchgeführt wird, ist ein sich wiederholender Vorgang. Es ist wichtig, dass es von Audit zu Audit nur inhaltliche Veränderungen gibt, aber keine strukturellen an der Methodik selbst. Dadurch wird gewährleistet, dass die Ergebnisse wiederholt durchgeföhrter Audits in sich stringent, vergleichbar und nachvollziehbar bleiben.

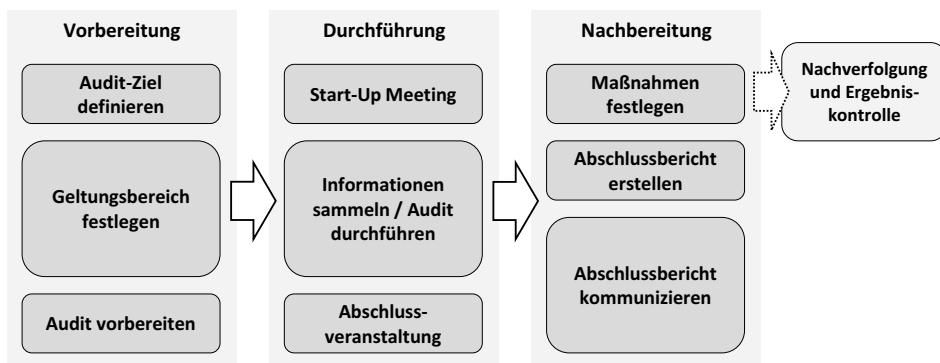


Abbildung 12.7: Exemplarische Durchführung eines Audits

Abbildung 12.7 zeigt exemplarisch auf, wie die Methodik der Durchführung eines Audits aussehen könnte. Jeder Block beinhaltet Einzelschritte und ist als solcher als Phase innerhalb des gesamten Prozesses zu verstehen. Nach dem Audit ist immer auch vor dem nächsten Audit: Audits bauen aufeinander auf,



und eine wichtige Größe, die den Output eines Audits und Input für eine folgende Prüfung darstellt, ist der Maßnahmenkatalog. Dieser listet aus Audits abgeleitete Maßnahmen auf und dokumentiert deren Fortschritt.

12.8.1 Vorbereitung

Mit der Definition der Ziele eines Audits beginnen die Vorbereitungen. Dazu gehört zunächst die Festlegung, um was für einen Audit-Typ es sich handelt. Es kann sich um ein Erst-Audit handeln, um ein wiederholtes Audit oder eine Überprüfung von einzelnen Maßnahmen, die in einem früheren Audit festgelegt wurden. Auch die Art des Audits muss festgelegt werden. Abhängig von der Art der untersuchten Bereiche kann es sich um rein technische Audits handeln, bei denen über Penetrationsversuche Schwachstellen gesucht werden, um ein Audit der Konfiguration von IT-Systemen, um die Prüfung formaler Sachverhalte wie den Stand von Awareness-Maßnahmen oder Zusätze zum Arbeitsvertrag oder um ein Prozess-Audit, das z.B. Datenflussanalysen enthält. Jede der aufgezählten Audit-Arten wird eine andere Vorgehensweise und eine andere Teamzusammensetzung bedingen und damit auch eine andere Vorbereitung.

Die nächste Festlegung betrifft den Umfang des Audits. Es gibt viele Definitionen, welchen Geltungsbereich ein Sicherheits-Audit typischerweise umfassen sollte. Die richtige Antwort darauf ist: »Es kommt darauf an.« Abhängig davon, inwieweit die interne Revision auch IT-Themen bearbeitet, abhängig vom Grad des Outsourcings, des Budgets, der verfügbaren Zeit, der Anzahl an Mitarbeitern und inwieweit der Datenschutzbeauftragte die Umsetzung von technisch-organisatorischen Maßnahmen selber kontrolliert, ist der Geltungsbereich größer oder kleiner. Dazu kommt die Frage, ob sinnvollerweise das gesamte Unternehmen betrachtet werden soll oder nur definierte wichtige Bereiche wie z.B. die Vorentwicklung oder das Rechenzentrum. Die Festlegung des Geltungsbereichs in der Vorbereitungsphase umfasst detaillierte Anleitungen, welche Prozesse, Funktionen, IT-Systeme etc. innerhalb der Prüfung untersucht werden und welche nicht.

Die Vorbereitungsphase wird damit abgeschlossen, die Informationen aus der Zieldefinition und der Definition des Geltungsbereichs als Grundlage für die Festlegung der Vorgehensweise beim Audit, die Art des Audits, die Fragenkataloge und die Teamzusammenstellung zu bestimmen. Richtlinien und andere Vorgaben, die als Grundlage dienen könnten, müssen identifiziert



und vorbereitet werden. Von diesen Informationen wird die Vorgehensweise bei der Prüfung maßgeblich abhängen.

12.8.2 Durchführung

Alles beginnt mit der ersten Besprechung. Dieses Start-up-Meeting ist dabei mehr als nur eine Teamfindungsveranstaltung. Dieser Termin wird auch genutzt, um die Festlegungen, die in der Vorbereitungsphase abgestimmt wurden, gemeinsam durchzugehen und ein Agreement darüber zu finden. Aus diesem Grund sollten neben den Teammitgliedern, die für die Audit-Durchführung verantwortlich sind, auch Personen aus höheren Leitungsebenen anwesend sein. Auf diese Art gewinnt die Prüfung den formalen Charakter, den sie benötigt, um eventuell auftretenden Problemen und Meinungsverschiedenheiten wirkungsvoll begegnen zu können. Das gilt vor allem dann, wenn sie eng mit finanziellen Ausgaben verknüpft sind. Dieser erste Termin sollte von der Zeitdauer und der Art der Moderation so angesetzt werden, dass die Inhalte besprochen werden können, ohne dass eine weitergehende Diskussion vom Zaun gebrochen wird. Eine Dauer von ca. 60 bis 90 Minuten hat sich als sinnvoller Zeitraum erwiesen.

Bei der Durchführung des Audits handelt es sich um den eigentlichen Hauptteil der Prüfung. Nun werden im Rahmen der getroffenen Festlegungen mit den Zielen der IT-Security und der Unternehmensführung Informationen gesammelt. Der Umfang und die Vorgehensweise bei diesem Schritt richten sich nach der Art der untersuchten Objekte und den im Unternehmen üblichen Methoden. Jede Information wird so dokumentiert, dass sie später als Grundlage für eine Aussage im Abschlussbericht dienen kann.

Auf die eigentliche Prüfung folgt der Abschlusstermin, der üblicherweise zusammen mit dem gleichen Personenkreis wie das Start-up-Meeting abgehalten wird. Es ist nicht das Ziel, detaillierte Auskunft über Befunde zu geben oder ein endgültiges Fazit zu ziehen. Das ist Aufgabe des Abschlussberichts. Dennoch kann zu diesem Zeitpunkt sicher eine Aussage über den Verlauf des Audits gemacht werden und ob die in der Vorbereitung getätigten Festlegungen über die Rahmenbedingungen durchweg sinnvoll waren. War dies nicht der Fall oder konnten aus irgendwelchen Gründen nicht alle avisierten Bereiche geprüft werden, so kann nun ein zeitnah erfolgendes Nach-Audit vereinbart werden.



Mitschrieb

Während der Durchführung eines Audits wird im Normalfall ein Mitschrieb angefertigt, der später als Datensammlung für den Abschlussbericht dient. Der Mitschrieb orientiert sich an den Fragenkatalogen und sollte jeweils protokollieren, wer welche Aussage zu welchem Thema gemacht hat. Dazu kommen die Interpretation des Auditors und seine eigene Einschätzung. Für den Fall von Kontroversen nach der Veröffentlichung des Abschlussberichts dienen die Mitschriebe als Protokoll der getätigten Aussagen und damit als wichtigste Grundlage für die Argumentation von Beschreibung und Bewertung der überprüften Bereiche.

Fragenkatalog

Ein Audit muss einer definierten Linie folgen, um sicherzustellen, dass keine Themen übergangen werden. Diesen roten Faden liefert im Allgemeinen ein Fragen- oder Themenkatalog. Anhand eines solchen Katalogs können Interviews genauso wie technische Tests strukturiert werden. Die Bandbreite reicht dabei vom lockeren Interview, bei dem der Auditor schriftlich diejenigen Aussagen festhält, die er für bemerkenswert erachtet, bis hin zu Fragenkatalogen über Hunderte von Fragen, die detailliert ausgefüllt werden müssen. Die zuerst genannte Vorgehensweise ist vor allem dann üblich, wenn ein Prüfer in einem Bereich tätig wird, in dem zwar die Vorgaben klar sind, das Umfeld aber komplett unbekannt ist und er sich zunächst einen groben Überblick verschaffen möchte. Denkbar wäre ein Audit eines physischen Raums wie z.B. eines Rechenzentrums. Liegen keine detaillierten Vorgaben über Maßnahmen wie Zugang, Brandschutz, Klimatisierung oder Verkabelung vor, so wird der Auditor zunächst die offensichtlichen Bedingungen prüfen. Das wären in diesem Fall Fragestellungen wie: »Sind Brandschutzmaßnahmen umgesetzt und wie gestalten sich diese?« Ein Vorgehen anhand eines Fragenkatalogs würde eher folgendermaßen aussehen: »Sind zwei Pulverfeuerlöscher in unmittelbarer Reichweite zum Hauptzugang des Rechenzentrums vorhanden?«

Wie bei allen Dokumentationen gilt auch bei der Zusammenstellung von Fragenkatalogen, dass ein Kompromiss zwischen Detaillierung und Aufwand gefunden werden muss. Ist ein Katalog zu umfangreich gestaltet, dann muss mehr Zeit für die laufende Pflege der Inhalte aufgewendet werden. Sind zu wenige Fragen vorgesehen, dann kann dies negative Folgen für das Sicherheitsniveau nach sich ziehen.



Ein weiterer Punkt ist ähnlich wie bei der Ermittlung von Kennzahlen die Art der Antwortmöglichkeiten. Diese können in schriftlicher Textform vorgesehen sein oder aber auch als binäre Antworten mit den Inhalten »ja« oder »nein«. Natürlich sind auch alle Schattierungen dazwischen denkbar. Die hier erforderliche Überlegung ist, dass Fragenkataloge, insbesondere wenn diese zahlreich vorliegen, elektronisch auswertbar sein sollten. In einem Unternehmen mit 25 Standorten möchte die Unternehmensleitung vielleicht wissen, welches Ranking diese untereinander in Bezug auf das Sicherheitsniveau haben und wie sich dieses in den letzten fünf Jahren verändert hat. Wenn nun Kataloge jeweils mit 100 Fragen und Antworten vorliegen und diese handschriftlich in Textform ausgefüllt wurden, vermutlich mit zusätzlichen Bemerkungen, dann wird der Aufwand höher sein, als wenn alle in Excel ausgefüllt wurden mit Antworten zwischen »kaum vorhanden« bis »vollständig«.

12

Zusammengefasst sollten folgende Bedingungen für Fragen und Antworten erfüllt sein, um einen guten Fragenkatalog zu ergeben:

- Klare und unmissverständliche Fragen. Keine doppelten Verneinungen oder kryptische Fragen.
- Das Niveau der Fragen sollte durchweg konstant bleiben.
- Richten sich die Fragen an gesetzliche Vorgaben, dann sollte dieser Hintergrund sinnvollerweise angegeben werden.
- Es muss unterschieden werden zwischen »muss« und »kann«. Beinhaltet Fragen eine Ausgangsfeststellung, so muss der Befragte wissen, ob das Geforderte ein Muss- oder ein optionales Kriterium ist.
- Antworten sollten so abgefragt werden, dass die Ergebnisse elektronisch verarbeitet werden können. Dabei kann es sich um schlichte »Ja/Nein«-Antworten handeln oder aber gestaffelte Antworten nach dem Schema Umsetzungsgrad 25%/50%/75%/100%.
- Nicht alle Fragen und damit auch alle Antworten sind gleich wichtig. Es sollte eine Möglichkeit vorhanden sein, Fragen in verschiedene Prioritätsklassen einzuteilen. Diese werden spätestens bei der Auswertung mit in die Berechnung aufgenommen.

Der Fragenkatalog sollte passend und klar strukturiert sein. Passend dahin gehend, dass die gestellten Fragen auf das untersuchte Gebiet passen und damit auch sinnvoll beantwortet werden können. Fehlinterpretationen sollten



EIN AUDIT SCHRITT FÜR SCHRITT

genauso ausgeschlossen sein wie die Konzentration auf eher unwesentliche Bereiche. So macht es wenig Sinn, Punkte extensiv zu hinterfragen, wenn die betroffenen Werte nur eine geringe Bedeutung für das Unternehmen haben.

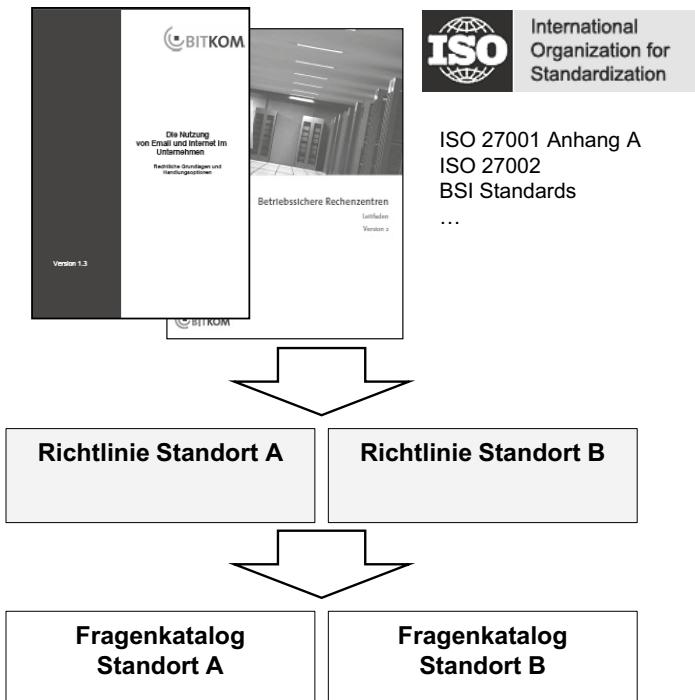


Abbildung 12.8: Quellen für einen Audit-Fragenkatalog

Es ist aus verschiedenen Gründen zu empfehlen, eigene Fragenkataloge von »offiziellen« Fragenkatalogen anerkannter Institutionen, die oftmals im Internet verfügbar sind, abzuleiten. Offensichtlich ist ein Grund der, dass nicht jeder über die Expertise verfügt, alle erforderlichen Punkte zu kennen und im Fragenkatalog abzudecken. Dazu kommt aber auch, dass die Nähe zu Standards immer sinnvoll ist – nicht zuletzt dann, wenn es um die Vergleichbarkeit geht. So stellen Organisationen wie der Verband der Automobilindustrie (VDA) einen Fragenkatalog bereit, den VDA-ISA-Katalog, an denen sich Mitglieder oder auch branchenferne Unternehmen in bestimmten Bereichen orientieren können. Nicht zuletzt helfen auch Normen wie die Grundsatzkataloge des BSI oder der Anhang A der ISO 27001 dabei, einen Fragenkatalog zu strukturieren und mit den entsprechenden Abfragen zu versehen.



12.8.3 Nachbereitung

Die Nachbereitung eines Audits kann in zwei Teile gegliedert werden. Zum einen ist der Abschlussbericht neben seiner Funktion, den Ist-Zustand aufzuzeigen, auch ein Gradmesser für das herrschende Sicherheitsniveau und stellt damit per se einen Auftrag zur Verbesserung dar. Als Zweites ist die Liste der gefundenen Abweichungen, die dem Abschlussbericht entnommen werden kann, ein formaler Auftrag, Projekte zu starten, Maßnahmen zu definieren und diese abzuarbeiten. Der Abschlussbericht steht damit auf der Stufe eines Pflichtenhefts aus dem Projektmanagement und sollte auch als solches gesehen werden. Die Abarbeitung der Maßnahmen im Rahmen von Projekten ist damit auch eine geeignete Vorgehensweise.

12

Die Präsentation des Abschlussberichts erfolgt regelmäßig im Rahmen einer Sitzung, zu der auch ein Teil der Teilnehmer des Audits anwesend sind. Naturgemäß kann es dabei zu Protesten und Einwürfen kommen, was die Inhalte des Berichts betrifft. Es macht keinen Sinn, diese Einwürfe in dieser Runde und zu diesem Zeitpunkt abzuarbeiten. Dies sollte später erfolgen, wenn der endgültige Bericht zur Kommentierung freigegeben wird. Aus diesem Grund sollte der Auditor sicherstellen, dass nur die Fragen, die von seiner Seite noch offen sind und noch nicht beantwortet werden konnten, durchgesprochen werden und der weitere Ablauf mit dem Abschlussbericht und der Zeitpunkt der Veröffentlichung kommuniziert wird. Ein kurzer Kommentar zum Ablauf und zum abgearbeiteten Umfang rundet den Termin ab.

Bevor der Bericht an alle im Voraus vereinbarten Stellen weitergegeben wird, sollte er zunächst abgestimmt werden. Es ist immer möglich, dass Daten fehlinterpretiert wurden, oder Aussagen, die mit einer gewissen Unschärfe vorgebracht wurden, missverstanden worden sind. Bevor also das Risiko eingegangen wird, dass sich die Konzentration nachher auf einen im Audit gemachten formalen Fehler verschiebt, sollte den Verantwortlichen die Möglichkeit gegeben werden, den Bericht durchzusehen und zumindest auf technischer Ebene abzusegnen. Im Anschluss daran kann der Abschlussbericht kommuniziert werden.

12.8.4 Abschlussbericht

Der Abschlussbericht fasst alle erfassten Abweichungen, deren Interpretation und Bewertung in einem Dokument zusammen. Zusätzlich enthält er oft Vor-



schläge für Maßnahmen, die der Auditor für erforderlich erachtet, um das angestrebte Sicherheitsniveau zu erreichen. Dieses Sicherheitsniveau muss im Vorfeld definiert worden sein. So ist es zumeist wenig sinnvoll, einen Standort von einem sehr laxen Niveau mit einem Schritt auf einen Spitzensitz bringen zu wollen. Abgesehen davon, dass dies kaum möglich ist und den Standortverantwortlichen überfordert, wäre es aus taktischen Gründen unklug. Es macht mehr Sinn, die gröbsten Probleme durch stringente Nachverfolgung von Maßnahmen zu bereinigen und eher schneller ein neues Audit anzusetzen. Dadurch ist es möglich, Fortschritte aufzuzeigen, sogenannte *quick wins*, und sich gleichzeitig auf die größten Risiken zu konzentrieren. Auf diese Weise kann die Motivation auf einem hohen Wert gehalten werden, und es besteht nicht die Gefahr, die Teilnehmer zu überlasten.

Hinweis

Während eines Audits werden die Abweichungen der Ist-Situation vom, z.B. durch Richtlinien definierten, Soll ermittelt. Werden Abweichungen gefunden, so werden diese dokumentiert und abhängig vom damit verbundenen Risiko bewertet. Welche konkreten Maßnahmen zur Risikobehandlung gewählt werden, wird üblicherweise von den zuständigen Experten der IT-Security oder IT festgelegt. Ob diese Maßnahmen ausreichend sind, wird wiederum von den Auditoren geprüft. Diese Wechselbeziehung soll die Gewaltenteilung zwischen den operativen Einheiten und der Audit-Organisation sicherstellen.

12

Ein Audit erfährt seinen Wert aus dem Abschlussbericht, der es verschiedenen Adressaten ermöglicht, den Ist-Zustand der IT-Security im Vergleich zum Soll-Zustand zu erkennen, und der die Entwicklung des Sicherheitsniveaus von Audit zu Audit aufzeigt. Vom Abschlussbericht werden Maßnahmen abgeleitet und deren Umsetzung im nächsten Audit wiederum überprüft. Damit betrifft dieser Bericht von der Unternehmensleitung abwärts alle Personen, die in irgendeiner Hinsicht in den Betrieb der geprüften Bereiche involviert sind. Gleichzeitig ist festzustellen, dass die Qualität des Berichts Aussagen über die Qualität der Prüfung an sich erlaubt. Ein fehlerhafter oder mehrdeutiger Abschlussbericht konterkariert alle Bemühungen, die in die Prüfung investiert wurden.



KAPITEL 12 – IT-SECURITY-AUDIT

Verschiedene Leser haben unterschiedliche Erwartungen an einen Audit-Bericht. Für die Unternehmensleitung wird üblicherweise ein Management-Überblick genügen, der stark vereinfacht den Sicherheitsstatus wiedergibt. Ein Mitarbeiter der IT-Abteilung hingegen wird auf die detaillierten Hinweise angewiesen sein, die wiederum zu Maßnahmen führen, deren korrekte Umsetzung von aussagekräftigen Anweisungen abhängig ist.

Adressaten eines Abschlussberichts sind damit alle Stellen, die für die geprüften Felder zuständig sind, die allgemein die Verantwortung tragen oder aber die für die Umsetzung von Maßnahmen und damit die Verbesserung des Sicherheitsniveaus Verantwortung tragen.

Ein Audit-Bericht weist mindestens die folgenden Inhalte auf:

12

- Geltungsbereich des Audits mit eventueller Abgrenzung, warum bestimmte Bereiche nicht Teil der Prüfung sind
- Zielsetzung des Audits
- Auflistung der Richtlinien, die als Basis herangezogen werden
- Verweise auf vorhergehende Audits und eine Übersicht über den Stand daran gekoppelter Maßnahmen
- Übersicht über alle Personen, die Teil des Teams waren und deren Aussagen in das Audit eingeflossen sind
- eine Managementübersicht über die wichtigsten Abweichungen bzw. Befunde (*findings*) und deren Priorisierung. Häufig wird dies in Form einer Farbskala oder mithilfe von Ampeln visualisiert.
- Kategorisiert nach Bereichen werden die Felder aufgeführt und die Ergebnisse des Audits dargestellt. Davon ableitbare Empfehlungen und (technische) Maßnahmen werden aufgeführt.
- Der Zusammenhang zwischen dem gefundenen Ist-Zustand und bestehenden Erwartungen, die aus Regelungen abgeleitet werden können, wird hergestellt.
- Die Einschätzung des Auditors
- Die Klassifizierung des Dokuments und damit die Festlegung, welcher Personenkreis darauf Zugriff erlangen darf

Der zentrale Teil des Berichts enthält die Befunde. Dabei handelt es sich um Abweichungen vom Soll-Zustand. Diese werden folgendermaßen beschrieben:



1. Eine Beschreibung des Befunds, wie er vom Auditor ermittelt wurde
2. Eine Darlegung, inwieweit der Befund vom angestrebten Soll-Zustand abweicht
3. Der Grund für den Befund. Dieser Grund kann darin liegen, dass eine bestehende Regelung oder eine Maßnahme nicht beachtet wurde oder eine Regelung oder Maßnahme trotz Einführung keine Abhilfe gebracht hat. Die Beschreibung der Regelung oder Maßnahme und die Umstände geben Hinweise darauf, wie zukünftig mit dem Befund umgegangen werden soll.
4. Der Befund wird quantifiziert. Dies findet mithilfe einer Klassifizierung statt, die aussagt, welcher Schaden entstehen kann, wenn der Befund nicht behandelt wird.
5. Ein Befund führt zu einem Risiko. Aus diesem Grund werden an dieser Stelle diejenigen Maßnahmen aufgeführt, die zur Verminderung des Risikos führen sollen.

Ein Bericht sollte nur die Informationen enthalten, die alle Parteien benötigen, um im Anschluss an die Veröffentlichung ihre Arbeit verrichten zu können. Zu ausführliche Berichte sind genauso wenig angebracht wie Berichte, die nur aus Stichworten bestehen und schwer zu deuten sind.





13 Management von Sicherheitsereignissen und IT-Forensik

13.1 Kapitelzusammenfassung

Das Management von Sicherheitsereignissen (Information-Security-Incident-Management) bzw. Sicherheitsvorfällen wird in der ISO 27035 beschrieben und dreht sich um den gesamten Komplex, der von der Planung eines Reaktionsteams bis hin zu einem vollständigen Melde- und Bearbeitungsprozess von Sicherheitsereignissen (*incident response process*) reicht.

Die IT-Forensik beschäftigt sich mit der Frage nach den Ursachen und Hintergründen eines sicherheitsrelevanten Ereignisses. Die meisten Ereignisse im Rahmen der IT-Security werden dabei Angriffe sein, die das Ziel haben, unerlaubten Zugriff auf Daten zu nehmen oder IT-Systeme zu sabotieren. Die Ergebnisse, die aus einer solchen Untersuchung gewonnen werden, helfen im weiteren Verlauf dabei, die korrekte Vorgehensweise als Reaktion auf den Vorfall zu entwickeln.

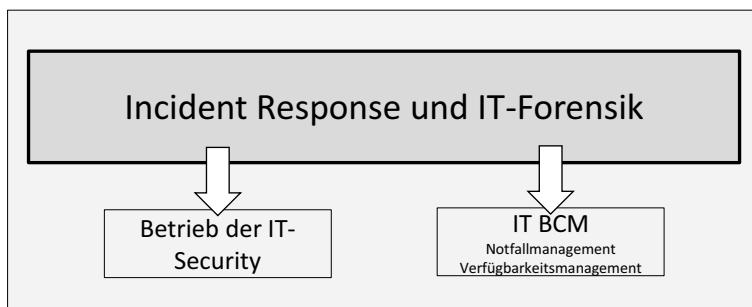


Abbildung 13.1: Primäre Abhängigkeiten von anderen Themen der IT-Security

Das vorliegende Kapitel beschäftigt sich mit dem Prozess, der mit der Implementierung eines Meldeprozesses von sicherheitsrelevanten Ereignissen beginnt und mit der Identifizierung von Beweisen endet.



Die Top-4-Fragen zum aktuellen Kapitel:

- Sind Prozeduren installiert, die es jedermann erlauben, sicherheitsrelevante Ereignisse zu melden?
- Existiert eine Stelle in der Organisation, die gemeldete Sicherheitsereignisse aufnimmt und verarbeitet?
- Wurden Vorbereitungen getroffen, im Falle eines Sicherheitsereignisses mit forensischen Mitteln darauf zu reagieren? Dies beinhaltet entsprechende Prozesse und Vorgehensmodelle.
- Ist den Mitarbeitern, insbesondere den Administratoren, bewusst, welche Möglichkeiten es gibt, Angriffe auf Daten des Unternehmens auszuüben, und worauf sie achten müssen, um solche Angriffe aufzudecken? Sind die Mitarbeiter informiert, sensibilisiert und wachsam?

13

13.2 Einführung

Ist ein Sicherheitsereignis (*information security incident*) eingetreten, das die Vertraulichkeit, Verfügbarkeit oder Integrität von Daten, Gebäuden, IT-Systemen, Produkten oder anderen Vermögenswerten gefährdet, dann ist es in erster Linie wichtig, davon umgehend Kenntnis zu erlangen, es professionell zu dokumentieren und alle Maßnahmen einzuleiten, es vollständig aufzuklären und zu beheben. Das Management von Sicherheitsereignissen ist dabei für die Erfassung und Verarbeitung zuständig, die Forensik für die tief greifende, oft technische Analyse der genauen Vorkommnisse.

Da sich Sicherheitsereignisse in ihrer Dringlichkeit und in ihrem Umfang von anderen Support-Fällen unterscheiden, beginnt der Prozess bereits bei der Hotline bzw. bei den Personen, die von Mitarbeitern angerufen werden, wenn Computerprobleme auftauchen oder wenn z.B. fremde Personen auf dem Unternehmensgelände gesehen werden. Im Fall von Ereignissen, die mit den IT-Systemen zu tun haben, wird die IT-Abteilung die erste Ansprechstelle sein, im Fall der Sichtung verdächtiger Personen oder eingeschlagener Fenster wird man sich eher an den Werkschutz wenden. Beide Ereignisse sind höchst unterschiedlich gelagert, könnten aber beide zu einem Abfluss von Know-how führen und müssen deshalb von einem Management von Sicherheitsereignissen erfasst und bearbeitet werden. Das Gleiche gilt für die Forensik. Bei Datendiebstahl sind unter anderem IT-Systeme zu untersu



chen, bei eingeschlagenen Fenstern sind z.B. Fingerabdrücke interessant. Beide Vorgehensweisen ähneln sich dahin gehend, dass sie das gemeinsame Ziel haben, die unmittelbare Gefahr zu bannen, gerichtsverwertbare Beweise zu sichern, das Vorgehen aufzuklären und daraus Schlüsse zu ziehen, welche Maßnahmen zur Reduzierung des Risikos zu ergreifen sind.

Den Anfang des Kapitels machen aber nicht die beiden titelgebenden Bereiche der IT-Security, sondern eine allgemeine Ausführung, woher Gefahren stammen können, die das Know-how des Unternehmens in Gefahr bringen. Ohne diese möglichen Angriffsvektoren zu kennen, ist der zielgerichtete Schutz der Vermögenswerte nicht möglich. Je nach Unternehmenszweck sind die zu schützenden Werte vor anderen Personengruppen zu schützen. Ein Rüstungsunternehmen wird die staatlich gelenkten Hacker im Auge haben, während ein Produktionsunternehmen darauf achten muss, dass nicht ein zufällig eingeschleppter Computerwurm die Produktionsmaschinen verschlüsselt und Lösegeld fordert. Abhängig vom Angriffsvektor und damit vom Angriff werden in der Folge sowohl der Meldevorgang als auch die Schwerpunkte der Forensik unterschiedlich ausfallen.

13.3 Angriffe auf Ihre Daten

Angriffe auf Unternehmen unter Nutzung von Computern ist nur eine weitere Art von Verbrechen. Auch hier liegen die gleichen Motive zugrunde wie bei anderen Straftaten auch: Bereicherung oder der Wille, Schaden anzurichten. Eine Spielart von »Er nimmt es den Reichen und gibt es den Armen« sind Angriffe mit dem Hintergrund, Informationen, die erlangt werden, offenzulegen oder vermeintlich »böse« Unternehmen zu bestrafen. Die Nutzung des Internets für einen Angriff senkt dabei die Hemmschwelle, da man das Opfer nicht direkt angeht, sondern nur indirekt über dessen IT-Infrastruktur. Das nachvollziehbare Bestreben, bei seiner Tat unerkannt zu bleiben, und die realistische Möglichkeit, dass dies über das Internet tatsächlich möglich ist, machen dieses Medium so beliebt. Dazu kommt natürlich die Möglichkeit, Angriffe über Länder- und Kontinentgrenzen hinweg zu verüben.

Die Begehung einer Straftat im Rahmen der Wirtschaftskriminalität, bei der IT-Systeme zum Einsatz kommen bzw. das Ziel darstellen, nennt man Computerkriminalität.



Hinweis

Die Kenntnis über mögliche Wege, Angriffe auf die Daten eines Unternehmens führen zu können, stellt die Grundlage für die Entwicklung möglicher Abwehrmaßnahmen dar. Das Melden von Sicherheitseignissen und die IT-forensischen Methoden orientieren sich demzufolge an den verschiedenen Angriffsmethoden.

13

Grundsätzlich muss zwischen internen und externen Angriffen unterschieden werden. Laut allen Umfragen der letzten zehn Jahre liegt dabei der Anteil von Computerstraftaten, die von den eigenen Mitarbeitern begangen werden, signifikant höher als diejenigen, die von Außenstehenden verübt werden. Mitarbeiter, die Daten stehlen, auf die sie sowieso Zugriff haben, haben dabei kaum ein Unrechtmachbewusstsein. »Ich habe diese Daten doch selbst erstellt« oder »Das habe ich selbst entwickelt«, hört man in diesem Zusammenhang häufig als Begründung. Deutlich verschärft wird die Motivation, diese Art Diebstahl durchzuführen, wenn der eigene Arbeitsplatz bedroht ist oder wenn bereits ein neuer Job in Aussicht steht. Ein Job, bei dem man die alten Daten gut gebrauchen kann.

Kulturell gesehen gibt es einige Länder, in denen es selbstverständlich ist, dass ein neuer Mitarbeiter nicht nur das Wissen in seinem Kopf mit in das neue Unternehmen einbringt, sondern auch so viele Informationen wie möglich in digitaler Form.

13.3.1 Durch eigene Mitarbeiter

Es ist statistisch vorhersagbar, welche Art von Angreifer ein Unternehmer mit einiger Wahrscheinlichkeit um sein Know-how erleichtern will. Am häufigsten werden es die eigenen Mitarbeiter sein. Gut geschult wissen sie am besten, welche Daten relevant sind, wo diese zu finden sind und wie die Sicherheitsmaßnahmen beschaffen sind. Sie wissen, wann samstags keiner mehr arbeitet, an welchem Rechner der USB-Port nicht gesperrt oder der Internetzugang nicht überwacht ist. Mit diesem Wissen alleine zählen Sicherheitsdienstleister bis zu 65 verschiedene Möglichkeiten auf, Daten aus dem Unternehmen zu schmuggeln. Die häufigsten sind dabei per E-Mail, auf externen Datenträgern wie USB-Sticks oder externen Festplatten, auf Mobiltelefonen



oder per Internet. Es ist ein Leichtes, anonym 50 Gigabyte freien Speicher im Internet zu bekommen. Der Upload geschieht per Browser, und die Übertragung ist verschlüsselt. Bis auf die Spuren auf dem lokalen Rechner und der reinen Aussage, dass dieser Rechner und dieser Benutzer eine Verbindung zu einem Anbieter einer Public Cloud mit Speichermöglichkeiten offen hatte, ist nichts nachzuweisen. Herrscht ein sehr hoher Sicherheitslevel, so werden Abwehrmaßnahmen dabei helfen, einen Anfangsverdacht zu formulieren. In den allermeisten Unternehmen wird diese Netzwerkverbindung nicht einmal bemerkt werden.

Im Fall des internen Mitarbeiters kann die Tat nur mit sehr hohem Aufwand verhindert werden. Hingegen kann aber erreicht werden, dass der Umfang des Diebstahls eng begrenzt wird. Dies ist dann möglich, wenn Benutzer nur auf die Daten Zugriff erhalten, die sie für ihre tägliche Arbeit auch wirklich benötigen. Selbst diese Zugriffe sind nur zu normalen Arbeitszeiten erforderlich, und es gibt weitere Möglichkeiten, den Zugriff einzuschränken. So sind Systeme in Unternehmen installiert, von denen immer nur eine vordefinierte Menge an Daten herunterkopiert werden kann. Der Versuch, größere Datens Mengen zu erhalten, endet mit einem Alarm.

Schon einfache Regeln, die in jedem Unternehmen umsetzbar sind, schränken den Umfang eines möglichen Datendiebstahls ein. Diese Regeln bilden die Grundlage und können durch entsprechende Maßnahmen technisch und organisatorisch stark ausgeweitet werden. Beispielhaft könnte eine solche Maßnahmenliste folgendermaßen aussehen:

- Zugriff nur auf Daten, die ein Mitarbeiter unbedingt benötigt
- Zugriffe auf alte Daten wie z.B. aus einem alten Projekt werden nur dann freigegeben, wenn diese aktuell noch erforderlich sind.
- Berechtigungen werden laufend hinterfragt und zeitnah angepasst.
- (Ungewöhnliche) Zugriffe auf Daten werden überwacht und untersucht. Dies rechnet man dem Bereich Verhaltensanalyse (*behavioral analysis*) zu.
- Mitarbeiter unterschreiben im Rahmen ihres Arbeitsvertrags eine entsprechende Klausel, die sie zur Geheimhaltung verpflichtet.
- Der Zugang zum Netzwerk und damit zu den Daten wird streng reglementiert.



Bei der Umsetzung solcher Regeln ist es sinnvoll, den Datenschutzbeauftragten hinzuzuziehen, da es sich um personenbezogene Daten handeln könnte, die im Rahmen der Erfassung von Protokolldateien gespeichert werden.

13.3.2 Durch Außenstehende

Bei externen Angreifern liegt die Aufgabe darin, die Latte höher zu hängen. Sprich, der Aufwand des Angreifers kann durch entsprechende Abwehrmaßnahmen in die Höhe getrieben werden. So schützt eine Firewall den Zugriff über das Internet und zwingt den Angreifer dazu, per lokalem Zugriff oder über Social Engineering tätig zu werden. Schulungen des Personals und gesicherte Netzwerkzugänge erhöhen die Sicherheit weiter, und der Angreifer wird zusätzliches Know-how benötigen, um diese Schranken zu überwinden. Dieses Zusammenspiel von Erhöhung der eigenen Sicherheitsmaßnahmen und Aufwand der Gegenseite kann beliebig weiter getrieben werden. Schlussendlich wird entscheidend sein, dass der Verteidiger stringent alle seine Systeme auf ein definiertes Sicherheitsniveau bringt. In diesem Szenario wird zumeist Nachlässigkeit an einer Stelle wie z.B. ein ungepatchter Server inmitten ansonsten aktueller Server den Zugriff durch den Angreifer ermöglichen. Im Grunde gilt weiterhin der bekannte Grundsatz, dass der Verteidiger immer alle Lücken schließen muss, wohingegen der Angreifer nur eine einzige finden muss, die er ausnutzen kann.

13.3.3 Angriffe und Angriffsvektoren

Der Angriffsvektor ist der Weg, den der Angreifer nimmt, um Zugriff zu einem Zielsystem zu erhalten. Die potenzielle Möglichkeit, den richtigen Angriffsvektor zu finden und eine geeignete Schwachstelle auszunutzen, bedeutet eine Bedrohung für das entsprechende System. Zu den bekanntesten Angriffsvektoren zählen Anhänge an E-Mails, Webseiten im Internet, Viren oder Trojaner. Gemeinsam haben diese Vektoren, dass sie auf Applikationen beruhen, die häufig mit sehr hohem Aufwand entwickelt wurden. Will man eine menschliche Schwachstelle ausnutzen, so reicht häufig genug bereits ein Telefonat als Angriffsvektor aus, um an die gesuchten Daten heranzukommen.

Firewalls haben in diesem Zusammenhang die Aufgabe, Angriffsvektoren abzublocken und den Angreifer davon abzuhalten, Angriffe auf verwundbare Systeme durchzuführen, also Systeme mit Schwachstellen, die nicht durch



entsprechende Maßnahmen auf das erforderliche Sicherheitsniveau gebracht wurden. Aber auch dieser Schutzmechanismus ist nicht vollkommen sicher, da es zum einen Möglichkeiten gibt, Firewalls zu umgehen, und des Weiteren kann es auch Schwachstellen auf Firewalls geben, die wieder einem Angriff ausgesetzt sein können.

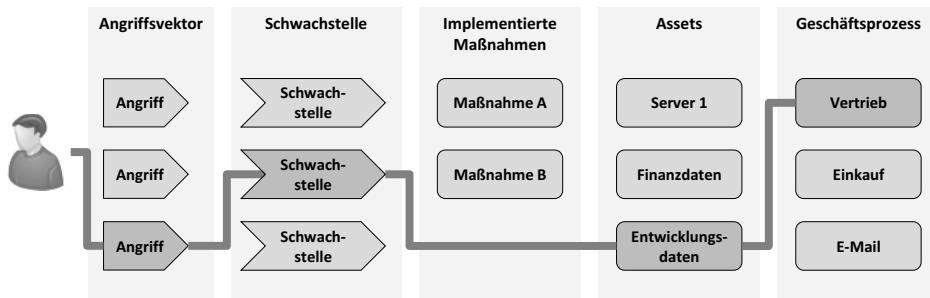


Abbildung 13.2: Angriffsvektor

13

In Abbildung 13.2 wird der Initiator als Person dargestellt, also wie der typische Hacker, der ein System zu kompromittieren versucht. Ist der Initiator eine Person, so muss von einer flexiblen Ausgestaltung des Angriffs ausgegangen werden. Dies reicht vom reinen manuellen Ausprobieren bis hin zu ausgefeilten Programmen, die viele mögliche Angriffspfade nacheinander austesten. Gesteuert werden beide Varianten von den Rückmeldungen, die sie jeweils erhalten. Ein »Zugriff verweigert« auf Systemebene kann schon ausreichen, dass die Person oder das automatisiert ablaufende Skript einen anderen Angriffsvektor nutzt. Aus diesem Grund ist die Verschleierung von Informationen über IT-Systeme und Applikation so wichtig.

Handelt es sich beim Initiator nicht um eine Person, sondern um ein Ereignis, so ist der Angriffsvektor leichter vorauszusehen. Für einen Initiator »Feuer« kann der Fachmann alle möglichen Eintrittsorte vorausschauen, mit einem Risikomanagement berechnen und Maßnahmen implementieren.

13.3.4 Angriffsarten

Unabhängig von der Art des Angreifers können verschiedenste Angriffsarten zur Anwendung kommen. Jede Art zielt auf eine Schwachstelle und auf ein Ziel. Der Diebstahl von Informationen beschränkt sich naturgemäß nicht ausschließlich auf das Ausspähen von Daten, sondern erstreckt sich genauso



auf Informationen, die in Papierform vorliegen. In den meisten Fällen wird es sich dabei um Informationen handeln, die ausgedruckt wurden, und aus diesem Grund ist es üblich, im Rahmen der Verhinderung von Angriffen auch diesen Weg des Informationsdiebstahls mit einzubeziehen. Im Grunde macht es auch keinen Unterschied, ob eine Kundenkalkulationstabelle als Datei vorliegt oder ausgedruckt als Stapel Papier. Im Folgenden werden verschiedene Angriffsarten erläutert.

Unangemessene Zugriffsrechte

Personen mit Zugriffsrechten, die sie nicht benötigen, aber aus den verschiedensten Gründen dennoch besitzen, sind eine der größten Gruppen potenzieller gefährlicher Angreifer. Dazu zählen Personen, die über die öffentliche Webseite an Daten gelangen, die sie nicht bekommen sollten, genauso wie Administratoren, die seit der Installation einer Applikation immer noch administrative Rechte darauf haben, oder Benutzer, die mehrmals innerhalb des Unternehmens die Stelle gewechselt und im Laufe dieser Zeit eine Vielzahl von Zugriffsrechten akkumuliert haben. Im englischen Sprachgebrauch spricht man bei Rechten, die ein Benutzer hat, ohne sie eigentlich zu benötigen, von *excessive privileges*. Insbesondere in Banken wurde dieses Problem frühzeitig erkannt. Ein Mitarbeiter, der vom Schalter in den Kundenservice und von dort in die interne Revision wechselt, hat im Laufe seiner Karriere völlig verschiedene Arten des Zugriffs besessen. Werden diese nicht konsequent nachgezogen, dann wäre er in die Lage versetzt, einen Diebstahl zu begehen, den er danach selbst untersuchen müsste. Ein solcher Fall wäre für das Image der Bank nachteilig. Um dieses Problem zu vermeiden, sind verschiedene GRC-Applikationen (Governance Risk and Compliance Software) erhältlich, die die Aufgabe haben, kollidierende Zugriffsrechte, die sich in einer Person vereinigen, aufzudecken. Geht man einen Schritt weiter, dann achtet man zusätzlich darauf, dass kritische Zugriffsrechte, wie z.B. das Recht zu bestellen und das Recht, den Wareneingang zu bestätigen, nicht in einer Abteilung liegen, um zu verhindern, dass sich zwei direkte Kollegen zu einer Straftat verabreden.

Social Engineering

Angriffe mittels Social Engineering sind in den Augen vieler eine der perfidesten Arten, einen Angriff durchzuführen. Grundsätzlich ist dabei die angegriffene Schwachstelle ein Mensch. Verschiedene bekannte Hacker haben



immer wieder demonstriert, wie sie ad hoc Daten stehlen können, ohne, abgesehen von einem Telefon, auf spezielle Hilfsmittel zugreifen zu müssen. Ein solcher Angriff kann so aussehen: Der Angreifer ruft in einem Unternehmen an und fragt nach der Telefonnummer eines IT-Mitarbeiters. Natürlich lässt er sich direkt verbinden, denn dadurch erscheint bei vielen Telefonanlagen bereits eine interne Telefonnummer beim IT-Mitarbeiter, und dieser vermutet einen Kollegen hinter dem Anruf. Mit ein wenig Interna fällt es dann deutlich leichter, diesen auch davon zu überzeugen. Von Kollege zu Kollege bittet er ihn nun um Zugriffsrechte, einen FTP-Zugang oder Ähnliches. Es ist erschreckend, wie hoch die Erfolgsquote solcherart Angriffe ist. Dazu kommt, dass bis zu diesem Stadium die völlige Anonymität des Angreifers sichergestellt werden kann. Es ist schon vorgekommen, dass ein IT-Mitarbeiter auf diesem Weg dazu gebracht werden konnte, Daten per DVD auf dem Postweg an den Angreifer zu verschicken.

Neben dieser Art des verschleierten Angriffs werden auch deutlich direktere Methoden wie Belauschung, Bestechung oder Drohung angewendet, um an Informationen zu gelangen. Wenn man bedenkt, wie weit das Abziehen von Informationen beim zufälligen Treffen in der Bar um die Ecke oder beim Mithören im Zug gehen kann, wird deutlich, dass diese Art des Angriffs sehr gefährlich ist und ihr mit entsprechenden Schulungsmaßnahmen begegnet werden muss.

Ein letztes Beispiel ist das sogenannte *masquerading*. Dabei handelt es sich um eine Art elektronisch unterstütztes Social Engineering. Eine E-Mail wird mit einem Absender versehen, den der Empfänger kennt, und an diesen verschickt. Mit einem Gefühl von Sicherheit wird er mit höherer Wahrscheinlichkeit die E-Mail öffnen und ein eventuell virusverseuchtes Programm starten, als wäre ihm der Absender unbekannt. Nicht umsonst weisen alle Stellen darauf hin, Programme von unbekannten Absendern sofort zu löschen und nicht zu starten. Dass dies natürlich auch für E-Mails mit bekannten Absendern gilt, sollte nicht unerwähnt bleiben. Ein weiteres Beispiel eines elektronisch unterstützten Social Engineerings ist der in den letzten Jahren massiv aufgekommene »CEO Fraud«. Dabei werden der interne E-Mail-Verkehr und die Befehlshierarchie im Unternehmen genutzt, um Mitarbeiter über finanzierte Anweisungen, in den meisten Fällen der Unternehmensleitung, zu Überweisungen von Geldbeträgen zu veranlassen. In anderen Fällen klinken sich Angreifer direkt in den gehackten Mailverkehr zwischen Kunde und Lie-



ferant ein und fälschen eine E-Mail, die die Zahlungsdaten enthält, z.B. indem sie eine gefälschte Kontonummer eintragen. Alle diese Angriffe werden mit sehr viel Aufwand vorbereitet und es wird immer schwieriger, echte E-Mails von gefälschten E-Mails zu unterscheiden.

Verwertung von Müll

Bislang hat die Digitalisierung nicht zum erwarteten papierlosen Büro geführt. Ganz im Gegenteil werden besonders wichtige Informationen heute extra ausgedruckt, um sie wertiger zu machen oder ablegen zu können. Diese Informationen, zusammen mit Unmengen an weniger wichtigen, landen regelmäßig im Papierkorb. Dessen Inhalt wiederum gelangt zumeist in eine Sammelstelle, bevor er dann abtransportiert wird. Diesen Müll nach verwertbaren Informationen zu durchsuchen, ist dementsprechend häufig ergiebig. Bei geheimen Informationen ist dies auf den ersten Blick einsichtig. Diese Papiere gehören in den Aktenvernichter. Bei den weniger wichtigen Informationen verhält es sich aber ebenso. Der Grund dafür liegt darin, dass mehrere unwichtig erscheinende Informationen zusammengenommen eine geheime Information ergeben könnte. Manchmal fehlt einem Angreifer nur ein Mosaiksteinchen, um einen erfolgreichen Social-Engineering-Angriff starten zu können. Das kann eine Telefonnummer eines IT-Mitarbeiters sein oder eine Glückwunschkarte, mit deren Informationen man einen trefflichen Aufhänger für ein Gespräch hätte.

Kleinvieh macht auch Mist

Wenn man in den Nachrichten von Datendiebstahl hört, dann geht es sehr häufig um Millionen von Datensätzen. Das lässt aufhorchen und die Nachricht verbreitet Angst. Das hat zur Folge, dass diese Taten mit höchster Energie und Aufwand verfolgt werden. Handelt es sich aber nur um wenige Datensätze und werden diese in unregelmäßigem Abstand gesammelt, so wird dieser Diebstahl oft genug überhaupt nicht bemerkt, und wenn es dann doch einmal passiert, dann hört man immer wieder den Spruch: »Wenn er nicht zu gierig geworden wäre, dann hätte man ihn nie erwischt.« Vermutlich ist diese Aussage sogar wahr. Einer der bekanntesten Fälle ist der, als in den 90er Jahren ein Programmierer in einer Bank bei jeder Überweisung immer einen Pfennig auf sein eigenes Konto überwiesen hat. Dies ging über mehrere Jahre gut, weil dieser Verlust alle internen Alarmierungsfunktionen, alleine aufgrund des geringen Betrages, unterschritten hat.



Diebstahl von Kennwörtern

Mit der Benutzerkennung und dem Passwort eines Kollegen Daten zu stehlen, löst mehrere Probleme auf einmal. Zum einen kommt man damit an Daten, auf die man selbst vielleicht keinen Zugriff hat, und zum zweiten wird der Verdacht nicht direkt auf einen selbst fallen. Alle Systeme, die auf eine Authentifizierung aufgrund von Benutzer und Passwort vertrauen, sind dahin gehend gefährdet und dementsprechend viele Möglichkeiten wurden entwickelt, um unberechtigt an diese Anmeldedaten zu gelangen.

Der einfachste Weg ist der, Passwörter zu erspähen. Das gelingt häufig genug beim Über-die-Schulter-Schauen oder indem man das Post-it unter der Tastatur findet, auf dem das Passwort vermerkt wurde. Der nächste Schritt besteht darin, elektronische Keylogger zu verwenden. Diese installiert man als Software oder – viel einfacher – man benutzt winzige Hardware, die man zwischen PC und Tastatur steckt und später wieder auswertet. Aufgrund der Tatsache, dass diese Geräte klein sind und sowieso niemand täglich sein Tastatkabel überprüft, ist dieses Vorgehen fast risikofrei.

Schwieriger wird es, wenn der Angreifer von außen kommt und es nicht schafft, bis zum Zielobjekt zu gelangen. In diesem Fall müsste er auf Trojaner oder andere Schadsoftware zurückgreifen. Aber auch hier gibt es Mittel und Wege: Studien zeigen, dass bis zu 45 % aller Benutzer, die auf dem Weg zur Arbeitsstätte einen herrenlosen USB-Stick finden, diesen an ihren Arbeitsplatzrechner anschließen, um den Inhalt zu erkunden. Also sind auch diese Herausforderungen lösbar.

Angriffe auf das Netzwerk

Ein Angriff auf die IT-Infrastruktur, die die Daten übermittelt, die man stehlen möchte, ist sehr naheliegend. Zudem ist der Zugriff auch ohne Benutzerkennung von außen möglich. Trotzdem gilt auch hier: Je näher man an den Daten ist und je mehr Informationen man über die Zielsysteme besitzt, desto einfacher wird der Angriff gelingen. In diesem Fall ist der direkte Angriff auf einen Datenserver aus dem Unternehmen heraus deutlich einfacher, als wenn zunächst die Firewall überwunden werden muss. Da Letzteres heute den meisten Angreifern nicht mehr möglich ist, verlegen sie sich häufig darauf, unbemerkt auf das Unternehmensgelände zu gelangen, sich direkt an das Unternehmensnetzwerk anzuschließen und von innen heraus die



Angriffe zu starten. Deshalb ist es auch so wichtig, die Firewall nicht als Grenze zwischen Unternehmen, da wo die Guten sind, und dem bösen Rest der Welt zu sehen. Jedes wichtige interne System, und dazu gehören sowohl die Server als auch die Netzwerkinfrastruktur, muss individuell vor Angriffen geschützt werden.

13.4 Management von Sicherheitsereignissen

Die ISO-Norm 27035 spricht von einem Computer Security Incident Response Team, abgekürzt »CSIRT«, wenn es diejenige organisatorische Stelle beschreibt, die in einem Unternehmen für die Aufnahme, Qualifizierung, Eskalation und Reaktion auf einen Sicherheitsvorfall verantwortlich zeichnet. In anderen Publikationen ist auch von einem Computer Emergency Response Team, einem »CERT«, die Rede. Es gibt keine einheitliche Meinung, worin die genauen Unterschiede zwischen einem CSIRT und einem CERT liegen. Im Folgenden schreiben wir von einem CSIRT, weil es die Verarbeitung von Ereignissen enger auf den Bereich der Sicherheitsereignisse eingrenzt. Ein weiterer Begriff, der sich bis heute nicht durchgesetzt hat, ist der des Information Security Incident Response Teams (ISIRT). Im Gegensatz zum CSIRT, das eine ganze Organisation beinhaltet, beschränkt sich dieser Begriff auf die Beschreibung des Teams an sich, das die Aufgabe des Managements von Sicherheitsereignissen wahrnimmt.

In wenigen Spiegelstrichen zusammengefasst sind die Hauptaufgaben eines CSIRT die folgenden:

- Ein CSIRT basiert auf einer Richtlinie, die die Aufgaben und Kompetenzen festlegt. Wie immer, wenn es um einen kontinuierlichen Verbesserungsprozess geht, ist es entscheidend, dass der beschriebene Gegenstand, in diesem Fall das Team, das hinter dem CSIRT steckt, durch geeignete Rückmeldungen laufend zur Weiterentwicklung der Prozeduren beiträgt.
- Das CSIRT entdeckt Sicherheitsereignisse entweder selbst, z.B. durch ein implementiertes SIEM oder durch Meldungen aus dem Security Operations Center (SOC) oder wird durch einen First-Level-Support, z.B. die Hotline, darauf aufmerksam gemacht. Wichtig ist dabei, dass die Meldung an sich vollständig ist und idealerweise auf einem definierten Formular basiert.



- Das CSIRT ist die erste Anlaufstelle, um die aktuelle Gefährdungslage abzufragen. Entscheidungsträger werden direkt durch das CSIRT über neue Risiken und den Stand alter Risiken aufgeklärt.
- Geht eine Meldung über ein Sicherheitsereignis ein, dann reagiert das CSIRT entweder selbstständig darauf und leitet die erforderlichen Maßnahmen direkt ein, oder aber es leitet das Ereignis, im besten Fall mit entsprechenden Empfehlungen versehen, an die verantwortliche Stelle, häufig die operative IT-Security, weiter.
- CSIRT-Mitarbeiter sind versiert in den Belangen der technischen IT-Security und bilden sich laufend weiter. Teil ihrer Aufgabe ist die präventive Untersuchung der IT-Landschaft auf mögliche Verwundbarkeiten. Daneben ist es ihre Aufgabe, Ereignisse, die an einer Stelle auftreten, darauf abzuprüfen, ob andere Teile der Infrastruktur in ebensolcher Weise gefährdet sind.

Wenn das CSIRT eine Meldung erreicht, dann kann es noch offen sein, ob der Angriff bereits vorbei ist, ob er erfolgreich war oder ob er noch im Gange ist. Die erste Handlung, die einer Risikoeinschätzung entspricht, ist die, festzustellen, ob Gefahr in Verzug ist und ob dementsprechend schnelle und entschiedene Maßnahmen erforderlich sind, um einer aktuellen, laufenden Gefährdung zu begegnen. Hat ein Angreifer unbemerkt einen Event auf einem Intrusion-Detection-System ausgelöst, dann muss verhindert werden, dass er weiterarbeiten kann. Nicht viele Unternehmen haben Abteilungen gebildet, in denen Experten rund um die Uhr erreichbar sind, eine solche Aufgabe zu bewältigen. Sehr viel häufiger werden externe Dienstleister hinzugezogen, um die Auswertung eines Vorgangs voranzutreiben und das Unternehmen hinsichtlich der zu treffenden Maßnahmen zu beraten. Aber selbst in diesem Fall muss zumindest eine Rumpfmannschaft definiert sein, die diese Maßnahmen auch umsetzen kann. Da es sich hierbei um technische Maßnahmen handeln kann, die Einfluss auf die Geschäftstätigkeit haben, wie z.B. die Abschaltung von Teilen des Netzwerks, müssen die benannten Personen nicht nur ein technisches Verständnis mitbringen, sondern auch die Kompetenz haben, schwerwiegende Entscheidungen zu treffen.

In 2018 ist ein Fall bekannt geworden, bei dem die eigentlich schon veraltete Schadsoftware WannaCry einen Großteil der IT-Systeme eines europäischen Unternehmens befallen hat. Dies blieb eine Zeit lang unbemerkt und die Software konnte erfolgreich ein sogenanntes Backdoor installieren, mit dessen



Hilfe es dem Angreifer ermöglicht wurde, Zugriff auf die Server und Clients zu nehmen. Das Unternehmen hat sofort nach Bekanntwerden externe Dienstleister hinzugezogen, die aber nicht feststellen konnten, welche Zugriffe erfolgt waren, welche Daten abgeflossen sind und welche weitere Schadsoftware in einem zweiten oder dritten Schritt zusätzlich installiert wurde. In diesem Fall war das Management auf ein solches Risiko vorbereitet und hat die Entscheidung getroffen, alle Clients und Server im Bürobereich herunterzufahren und neu zu installieren. Rechner in der Produktion wurden weiter betrieben, aber vom Netzwerk getrennt. Diese Entscheidung wurde schnell und kompromisslos getroffen und damit wurde das Risiko des Datenabflusses minimiert. Ein Unternehmen muss immer so weit vorbereitet sein, dass auch die Unternehmensleitung fachlich in der Lage ist, das Risiko eines solchen Angriffs gegen das Risiko der Beeinträchtigung des Geschäftsbetriebs abzuwagen und die erforderlichen Entscheidungen zu treffen. Das CSIRT wiederum hat dabei die Aufgabe, die Informationen bereitzustellen, die das Management benötigt, ein solches Risiko bewerten zu können.

13.5 IT-Forensik

Einer IT-forensischen Untersuchung geht immer ein Ereignis voraus. Manchmal handelt es sich um einen Angriff von außen auf die IT-Systeme, der aufgeklärt werden muss, um den Angreifer zu identifizieren oder zumindest um sicherzustellen, dass keine weiteren Angriffe mehr drohen. Häufig wird es sich dabei um ein internes Problem handeln. Ein Mitarbeiter hat auf Daten zugegriffen, auf die er nicht zugreifen darf, Mobbing hat stattgefunden, indem E-Mails mit unangemessenem Inhalt verschickt wurden, oder ein Wäschetrockner wurde zur Adresse eines ungeliebten Kollegen geordert. Neben der Technik und den Zielsetzungen spielt auch die persönliche Motivation des Täters eine große Rolle. Zur Erkennung des Gesamtproblems und zu dessen Eindämmung ist es wichtig, dies zu erkennen.

Die IT-Forensik ist ein Werkzeug, das auf vielfältige Art und Weise eingesetzt werden kann. Sie ist Bestandteil der Abarbeitung von gemeldeten Sicherheitsereignissen, aber auch der Behebung von Störfällen, deren Ursache noch völlig ungeklärt ist. Sie kann neben den genannten Einsätzen als Reaktion auf ein Ereignis auch ohne direkten Anlass genutzt werden. So macht es durchaus Sinn, eine Untersuchung aller Server auf Rückstände von Hackertools wie



Root-Kits durchzuführen. Dazu durchforsten kleine Programme oder Skripte die Dateiverzeichnisse und suchen nach typischen Rückständen an Dateien, die auftreten, wenn sich Angreifer der Kontrolle von IT-Systemen bemächtigt haben. In diesem Fall investiert ein Unternehmen Geld für die Suche nach etwas, das es vielleicht nicht gibt, und erwartet daraus Rückschlüsse, ob das Unternehmen in der Vergangenheit angegriffen wurde, inwieweit das aktive Monitoring funktioniert und falls ein Angriff festgestellt wird, wer der Urheber sein könnte. Erfahrungsgemäß ist der Aufwand einer solchen Untersuchung nicht groß, wenn aber etwas gefunden wird, das z.B. auf Wirtschaftsspionage hindeutet, kann sich die IT-Security der Aufmerksamkeit der Unternehmensleitung gewiss sein.

Jedes positive Ergebnis einer forensischen Untersuchung deckt das Vorhandensein von Risiken auf. Diese fließen wiederum in das IT-Risikomanagement und können, je nach Schweregrad, zu einer Neubewertung führen. Ein einfaches Beispiel ist die Erkenntnis, dass mit der Ausführung von Programmen, die Benutzer aus dem Internet herunterladen, Schadsoftware auf den Rechner gelangen kann. Wird durch eine forensische Untersuchung der gesamte Prozess vom Zugriff auf eine entsprechend präparierte Webseite über den Download bis hin zur Installation und Ausführung des Schadcodes nachgewiesen und visualisiert, dann rückt ein solch offensichtliches Problem schnell in den Fokus – etwas, das häufig genug nicht geschieht, wenn nur vage Vermutungen vorliegen. Eine Maßnahme mit Auswirkungen auf jeden Benutzer wäre in diesem Fall die Implementierung eines Betriebssystemfeatures, das die Ausführung unbekannter Dateien grundsätzlich unterbindet.

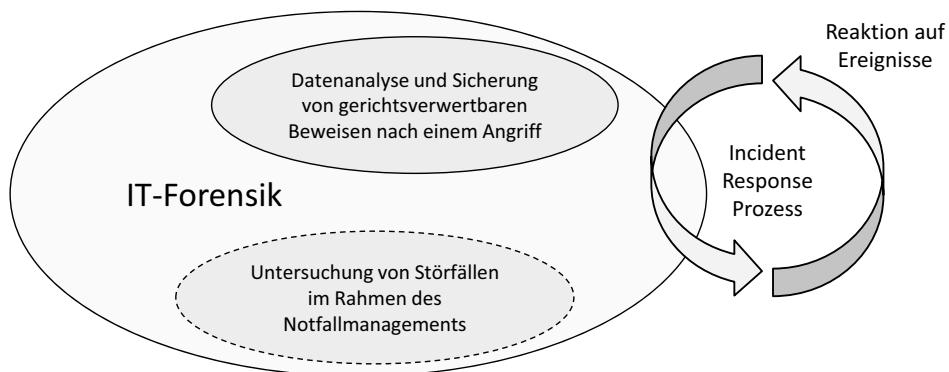


Abbildung 13.3: Die zwei Bereiche der IT-Forensik



KAPITEL 13 – MANAGEMENT VON SICHERHEITSEREIGNISSEN UND IT-FORENSIK

Wie in Abbildung 13.3 dargestellt, beinhaltet die IT-Forensik nicht nur die Untersuchung von Vorfällen, die zeitnah auf einen Angriff erfolgt. Die Vorgehensweise, also das Anstoßen des Meldeprozesses von Sicherheitsvorfällen, die Analyse von Daten und die daraus zu ziehenden Schlussfolgerungen lassen sich auch auf Störfälle anwenden. In vielen Fällen ist zum Zeitpunkt einer Alarmierung nicht sicher, ob es sich um einen Angriff oder eine technische Störung handelt. Ist z.B. die Unternehmens-Firewall zu 100 % ausgelastet, so kann es sich um einen Sicherheitsvorfall handeln, bei dem z.B. ein Virus im lokalen Netz die Firewall penetriert, einen Angriff aus dem Internet oder aber um einen Software- oder Hardwarefehler an der Firewall. Erst die Ereignisse der forensischen Untersuchung zeigen, ob der IT-Notfallmanagementprozess gestartet werden muss, oder aber die Abwehr eines Angriffs zu erfolgen hat.

13

Hinweis

Dieses Kapitel behandelt das Management von Sicherheitsvorfällen und den Forensikprozess. Die Behandlung im Rahmen eines IT-Notfallmanagements oder die Vorsorge mit technischen Mitteln des Continuity Managements werden in den entsprechenden Kapiteln behandelt.

Wie bereits erwähnt, beschäftigt sich die IT-Forensik mit der streng formal und streng methodisch durchgeführten Datenanalyse von Datenträgern oder von Informationen, die aus dem Netzwerkverkehr gewonnen werden können, und dient der Aufklärung von Ereignissen bzw. Vorfällen. Die beiden Worte »streng« und »formal« sollen in diesem Kontext unterstreichen, dass die Erfassung von Beweisen, vor allem wenn diese gerichtsverwertbar sein sollen, ein Vorgang ist, der nachvollziehbar und jeglicher kritischer Überprüfung standhalten muss. Aus diesem Grund beschreibt das Management von Sicherheitsereignissen (*Information-Security-incident-Response-Prozess*) jeden einzelnen Schritt mit der Zielsetzung, letztendlich feststellen zu können, was genau passiert ist, wer der Angreifer war und wie dies bewiesen werden kann. Von den Ergebnissen werden, basierend auf der Risikoeinschätzung, Maßnahmen abgeleitet und nach deren Umsetzung kann das Restrisiko ermittelt werden. Wie bei jeder Risikobehandlung steht dabei die Abwägung von Risiko und Chance im Mittelpunkt.

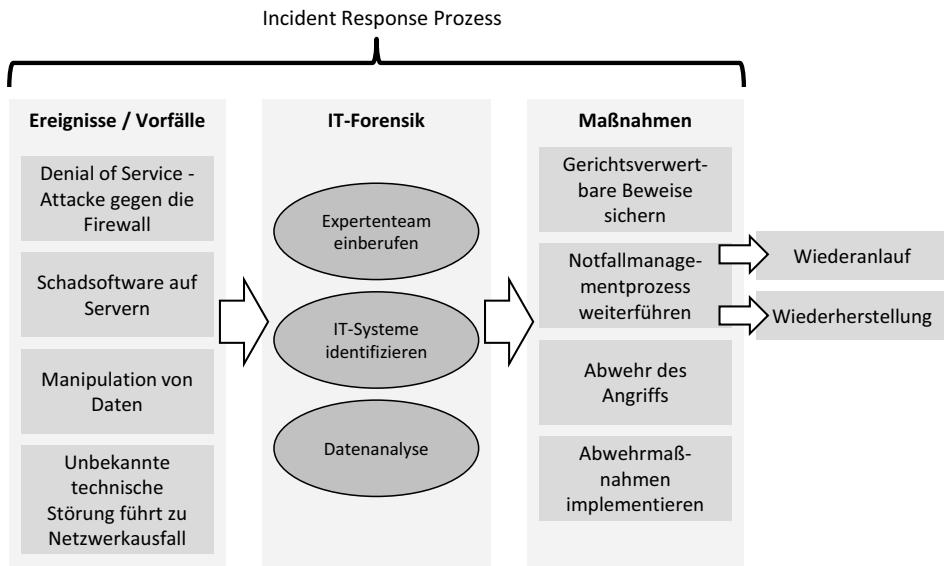


Abbildung 13.4: Incident-Response-Prozess

Ein Kernelement der technischen Umsetzung der IT-Forensik ist die Sicherstellung, dass die Informationsträger, aus denen Daten zur Datenanalyse extrahiert werden, in einem Zustand vorliegen müssen, der die nachträgliche Veränderung, bzw. Manipulation verhindert. Um vor Gericht beweisen zu können, dass eine Person eine bestimmte Tat ausgeführt hat, muss auch die Integrität der Beweise nachvollziehbar sichergestellt sein – dafür steht der Begriff der Beweismittelkette (*chain of custody*). Methodiken, um dies zu erreichen, sind die formale Dokumentation, die strikte Einhaltung der im Vorhin definierten Prozessschritte und die Sicherstellung, dass Beweise nicht verändert werden. Insbesondere der letzte Punkt ist essenziell, da sich ein Fehler an diesem Punkt nicht mehr korrigieren lässt. So ist es im Rahmen der IT-Forensik üblich, z.B. im Falle der Analyse von Daten auf einer Festplatte vor dem Start der Untersuchung eine exakte Kopie der Platte anzufertigen und das Original nicht anzutasten.

Hinweis

Der Incident-Response-Prozess beginnt zu dem Zeitpunkt, an dem ein Ereignis bemerkt wird, bzw. wenn ein solches gemeldet wird. Das Wort



response zeigt bereits, dass es sich dabei um eine Krisenreaktion handelt, und damit lässt sich dieser Vorgang, wenn man es aus Sicht des IT-Notfallmanagements betrachtet, der Krisenbewältigungsphase zuordnen.

In Abbildung 13.4 wird dargestellt, dass die IT-Forensik sowohl dazu dient, *nach* einem IT-Security-Vorfall Daten zu erheben und zu analysieren, als auch *während* eines Störfalls. Der Zweck der Datenerhebung ist dabei unterschiedlich und damit auch die Vorgehensweise. Ein Systemausfall aufgrund eines Softwarefehlers wird im Detail anders zu beheben sein als ein Angriff auf Schwachstellen einer Software. Was gleich bleibt, ist das Objekt der Untersuchung und damit auch die externen Ansprechpartner oder im Zweifelsfall auch die für diesen Fall geplanten Notfallmaßnahmen wie die Weiterführung des Betriebs durch Starten eines Notfallbetriebs.

13

Die Datenanalyse findet im Normalfall während der gesamten Zeitdauer der Krise statt und endet damit erst, wenn der Normalbetrieb wieder gestartet wurde. Der Abschluss der Dokumentation und die Diskussion, wie das Ereignis vermeidbar gewesen wäre und welche Maßnahmen erforderlich sind, um die Wahrscheinlichkeit zu vermindern, dass ein ähnlicher Vorfall erneut eintritt, werden üblicherweise zum Ende des Vorfalls gestartet.

Tritt ein Ereignis ein, das hohe Kosten verursacht, so wird neben der Frage, wie schnellstmöglich ein Notfallbetrieb etabliert werden kann, auch die Klärung im Raum stehen, wer dafür verantwortlich ist. Angenommen, der Vorfall besteht in der Manipulation von Produktdaten. In diesem Fall wird jeder Schritt der forensischen Untersuchung auch dazu dienen, Beweise zu sammeln, die zur Strafverfolgung genutzt werden können. Damit verschärfen sich die Spielregeln der Datenanalyse enorm. Um gerichtsverwertbare Beweise präsentieren zu können, muss ausgeschlossen werden, dass Daten im Laufe der Analyse verändert wurden. Diese Vorgabe legt die Rahmenbedingungen für den gesamten Prozess der IT-Forensik fest und damit auch für die Aktionen, die getätigten werden können. Der Fachbereich wiederum wird darauf bestehen, dass die Daten schnellstmöglich wieder zur Verfügung stehen, um den reibungslosen Betrieb wieder aufnehmen zu können. In diesem Spannungsfeld kommt es darauf an, dass zum einen die Vorgehensweise für solche Ereignisse festgelegt wird, und zum anderen, dass die Leitungsebene in den Prozess mit einbezogen wird.



13.5.1 Arten der IT-Forensik-Analyse

Die IT-Forensik stützt sich im Wesentlichen auf die Analyse von Daten, die entweder auf Datenträgern oder im Hauptspeicher vorliegen oder aber innerhalb eines Netzwerks gesammelt werden. Im täglichen Betrieb wird es sich also vorrangig um die Untersuchung von Festplatten von Arbeitsplatzrechnern, Servern, Maschinensteuerungen, aktiven Netzwerkkomponenten, Mobiltelefonen, Tablets oder aber Kommunikationsmitschnitte (*captures*) aus dem Netzwerk handeln. Die Analyse der dabei gewonnenen Informationen bildet die Grundlage der forensischen Bemühungen.

Abhängig vom Zeitpunkt der forensischen Analyse wird zwischen Post-mortem-Analyse und Live-Forensik unterschieden. Die Post-mortem-Analyse, auch Offline-Forensik genannt, befasst sich, wie der Name schon aussagt, mit der nachträglichen Analyse. Zu einem Zeitpunkt also, wenn das Ereignis bereits in der Vergangenheit liegt und flüchtige Speicher wie der Hauptspeicher bereits nicht mehr zugreifbar sind. In diesem Fall spricht man auch von der »Post-mortem-Spurensuche«. Dieser Begriff trifft es ganz gut. Nach Sicherstellung aller betroffenen IT-Systeme, was in einem produktiven Umfeld oftmals nicht problemlos möglich ist, werden vorhandene Datenträger auf Spuren untersucht. Die Spurensuche kann in diesen Fällen alle Ebenen von Applikationsdaten über Benutzerdaten bis hin zu Systemdateien umfassen.

Im Falle der Live-Forensik oder Online-Forensik beginnt die forensische Untersuchung zu einem Zeitpunkt, zu dem neben den nicht flüchtigen Speichermedien wie Festplatten auch flüchtige Speicher wie Caches auf Netzwerkgeräten oder der Hauptspeicher ausgelesen werden. Neben Speicherbausteinen, die ausgelesen werden können, besteht häufig auch Zugriff auf laufende Prozesse und Applikationen sowie auf temporäre Dateien, die Programme während der Laufzeit speichern. Der Vorteil einer Online-Analyse besteht darin, dass nicht nur die Spuren eines Ereignisses in Form von Datenfragmenten und Protokolldateien untersucht werden können, sondern dass der komplette Systemzustand zur Untersuchung zur Verfügung steht. Das beinhaltet laufende Applikationen, offene Dateien und häufig auch Passwörter und Dateien im unverschlüsselten Zustand im Speicher, die normalerweise nur verschlüsselt vorliegen. Auf der anderen Seite bestehen einige Nachteile, die wiederum die Vorteile einer Offline-Analyse sind: Das IT-System kann nur



vor Ort untersucht werden, und jeder Einsatz eines Tools bewirkt automatisch eine Zustandsänderung im System.

13.5.2 Einrichtung von Honeypots

Die Reaktion auf einen Sicherheitsvorfall unterscheidet sich in einigen Punkten von der auf einen Störfall. So steht im Rahmen eines Angriffs neben der Beweisführung auch die Ermittlung des Täters im Vordergrund. Soll dieser zweifelsfrei festgestellt werden, so ist es häufig erforderlich, diejenige Person während der Tat zu beobachten. Bei Angriffen auf die Firewall werden dazu Maßnahmen eingeleitet, um die Ursprungsadresse des Angreifers festzustellen. Dafür ist es erforderlich, den Angreifer zunächst gewähren zu lassen, und dies widerspricht den Grundsätzen des IT-Notfallmanagements, das dem Schutzziel Verfügbarkeit verpflichtet ist. Aus diesem Grund werden abgeschottete Bereiche innerhalb der Infrastruktur aufgebaut, sogenannte Honeypots für Computer oder Honeytokens für Softwareprodukte wie Webserver, die einen Angreifer anlocken sollen, ohne dass dieser Schaden anrichten kann. Ist der Angreifer auf einem so präparierten System aktiv, so kann er ohne Gefahr für den Betrieb beobachtet und sein Vorgehen analysiert werden.

Neben ganzen IT-Systemen, die einem potenziellen Angreifer als lohnenswertes Ziel angeboten werden, setzen Unternehmen auch Agenten zusätzlich zu Intrusion-Detection-Systemen ein, die günstig sind und in großer Zahl im Unternehmensnetzwerk platziert werden können. Diese werden aktiviert, sobald ein Angreifer typische Kontaktversuche auf den üblichen Ports vornimmt. Da diese Systeme keinen anderen Zweck verfolgen und nicht Bestandteil der aktiven IT-Infrastruktur sind, ist jeder Kontaktversuch zumindest verdächtig. Auf diese Weise lassen sich Port-Scans oder Schadsoftware, die sich verbreiten möchte, detektieren.

Alle genannten Methoden haben den Zweck, Visibilität zu schaffen. Eine Gefahr, von der man nicht einmal weiß, dass sie existiert, birgt das höchste Risiko, und Transparenz ist die einzige Möglichkeit, diesem Problem zu begegnen. Nicht zuletzt hilft es dem Manager IT-Security, wenn er darstellen kann, dass das Unternehmen tatsächlich gefährdet ist und es sich nicht nur um ein theoretisches Problem handelt.



13.6 Elemente der forensischen Untersuchung

Eine Meldung über einen sicherheitsrelevanten Vorfall geht ein, und es muss reagiert werden. Der Manager IT-Security, der unter den Ersten ist, der die Nachricht empfängt, weiß noch nicht, ob es sich um einen Angriff oder einen Systemfehler handelt. Er weiß aber genau, dass er, wenn die Meldung »Daten wurden im Personalsystem gelöscht« erscheint, davon ausgehen muss, dass ein Ereignis aufgetreten ist, das ein Angreifer auslöst. Aus diesem Grund wird er (zumindest, bis er weiß, ob es sich nicht doch um einen Softwarefehler handelt) alles tun, um keine Spuren zu zerstören. Kurz, er macht dann alles richtig, wenn er Punkt für Punkt den normierten Verhaltensregeln folgt.

Tipp

Für die Erstellung einer eigenen Vorgehensweise kann der »Leitfaden IT-Forensik« des BSI auf mehr als 350 Seiten wichtiges Fachwissen vermitteln. Einige Beispiele runden die Erläuterungen ab.

13

Die Rahmenbedingungen werden in den Richtlinien zur IT-Forensik festgehalten und beschreiben die formal methodische Vorgehensweise zur forensischen Untersuchung. In Abbildung 13.5 ist die Vorgehensweise in Schritten abgebildet.

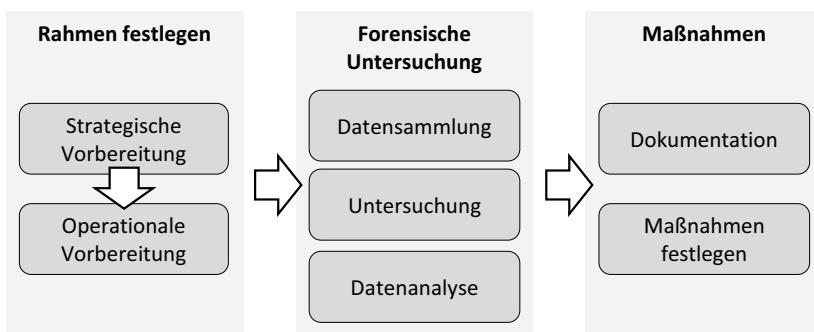


Abbildung 13.5: Vorgehensweise bei der forensischen Untersuchung

Der Abschlussbericht, der häufig auch als Basis für die Durchführung personalrechtlicher Konsequenzen dient, hat als Adressaten die Unternehmenslei-



tung, und nicht zuletzt aus diesem Grund ist es erfolgskritisch, dass die entsprechenden Leitungsebenen in den gesamten Prozess involviert sind. Handelt es sich um personenbezogene Daten, so ist selbstverständlich auch der Datenschutzbeauftragte mit einzubeziehen. Die Kommunikation zwischen den beteiligten Parteien ist immanent wichtig und sollte grundsätzlich als Teil des Beweissicherungsprozesses dokumentiert werden.

Wir gehen in diesem Kapitel von einem sicherheitskritischen Vorfall aus. Damit entfallen diejenigen Schritte, die bei einer technischen Störung angestoßen werden würden.

13.6.1 Zielsetzung

13

Die forensische Untersuchung muss in einer Art erfolgen, dass die angestrebten Ergebnisse erreicht werden können. So kann eine Kontaminierung von Spuren je nach Zielsetzung bereits dazu führen, dass der letztendliche Bericht unbenutzbar wird. Zu wissen, was man mit der Untersuchung schließlich erreichen möchte, ist damit der Schlüssel für die Vorgehensweise und entscheidet somit auch über den Aufwand und die Schritte, die unternommen werden sollen.

Die folgenden Fragen werden üblicherweise gestellt, wenn eine forensische Untersuchung stattfinden soll:

- Was ist geschehen?
- Wie ist es passiert?
- Wo ist es passiert?
- Wann ist es passiert?
- Wer hat es verursacht oder wer hat es getan?
- Welche Maßnahmen müssen getroffen werden, um eine Wiederholung zu verhindern?

Die aufgeführten Fragen führen zu einer schlichten Tatsache: Das Ziel einer forensischen Untersuchung ist es, die Wahrheit herauszufinden. Es geht nicht um die Bestätigung von Mutmaßungen, die im Vorfeld angestellt wurden.



Wichtig

Objektiv an eine forensische Untersuchung heranzugehen, ist eine wichtige Voraussetzung. In jedem Fall muss allen Hinweisen nachgegangen werden, ob diese für oder gegen den Angreifer bzw. Verursacher sprechen.

Je größer der Erfahrungsschatz eines Ermittlers ist, desto schneller wird er das Gefühl haben, dass er auf Anhieb weiß, was passiert ist, und auch dementsprechend ermitteln. Aus diesem Grund ist es wichtig, immer aufs Neue für sich selbst festzustellen, dass kein Fall so ist wie ein anderer in der Vergangenheit und dass der erste Schein häufig trügt. Fehlt diese Einsicht, dann kann es vorkommen, dass Spuren übersehen oder falsch interpretiert werden. Das führt in der Folge dann dazu, dass auch alle davon abgeleiteten Schlussfolgerungen in die falsche Richtung führen können.

13

13.6.2 Anforderungen an die Analyse

Die Zielsetzung, herauszufinden, wer etwas verursacht hat und wie es geschehen ist, zeigt bereits, dass es darum geht, Beweise für das unter Umständen kriminelle oder grob fahrlässige Handeln einer Person zu finden. Beweise wiederum müssen naturgemäß unzweifelhaft und unangreifbar sein. Um dies zu gewährleisten, folgt auch die Durchführung der Analyse strengen Regeln.

- Alle Schritte, die während der forensischen Untersuchung verfolgt werden, müssen peinlich genau dokumentiert werden. Dazu genügt es nicht, nur die technischen Aspekte zu dokumentieren. Auch die beteiligten Personen, eventuelle Zeugen, die Uhrzeit und die verwendeten Werkzeuge sollten niedergeschrieben werden. Der Abschlussbericht sollte von Personen aus dem Bereich des Betriebsrats und der Personalabteilung bezeugt werden.
- Alle Untersuchungen, die eine Veränderung der gesicherten Daten zur Folge haben könnten, sollten anhand einer bitgenauen Kopie vorgenommen werden. Damit soll vermieden werden, dass eine Verfälschung der Daten stattfinden kann und dass die Daten im Zuge der technischen Ana-



lyse verändert werden. Die Wahrung der Integrität der Daten muss während der Analyse und auch im Anschluss daran nachweisbar sein.

- Werden die Quelldaten während der Untersuchung verändert (dies ist z.B. in Fällen, bei denen der Arbeitsspeicher im Betrieb analysiert werden muss, nicht ausgeschlossen), dann müssen die Veränderungen dokumentiert werden. Den lückenlosen Nachweis über den Verbleib von digitalen Spuren und der daraus gewonnenen Schlussfolgerungen nennt man *chain of custody*.
- Ein Ergebnis muss im Zweifelsfall auch in einer juristischen Auseinandersetzung Akzeptanz finden. Das bedeutet, dass auch ein von der Gegenseite hinzugezogener Gutachter zu den gleichen Schlussfolgerungen kommen muss. Um dies zu erreichen, sollten alle Methoden und Werkzeuge einem in der Fachwelt akzeptierten Standard entsprechen.
- Eine Wiederholung der in der Dokumentation niedergeschriebenen Schritte muss immer wieder zu den gleichen Ergebnissen führen. Aus dieser Anforderung heraus ergeben sich die Rahmenbedingungen für die Qualität der Dokumentation, der verwendeten Werkzeuge und der Behandlung der ursprünglichen Daten.
- Die Vorgehensweise der Analyse muss in einer Art und Weise erfolgen, dass zum einen die Zielsetzung immer im Auge behalten wird und dass zudem der Zusammenhang zwischen den gefundenen Beweisen und den Ereignissen logisch nachvollziehbar ist.

13.6.3 Forensische Methoden

Für die Erfassung, Untersuchung, Analyse und Bewertung von Daten im Rahmen der forensischen Analyse stehen verschiedene Werkzeuge und Methoden zur Verfügung. Auch die Art der strategischen Vorbereitung spielt eine große Rolle, da unter Umständen bereits entsprechende Aufzeichnungen vorhanden sind, da proaktiv für das Ereignis vorgesorgt wurde.

In den meisten Fällen wird sich die Analyse auf das Betriebssystem und das Dateisystem sowie die von diesen Komponenten erzeugten Daten stützen. Damit wird aber auch gleichzeitig deutlich, dass dadurch auch die Grenzen gezogen werden, was möglich ist und was nicht. Daten, die in der Vergangenheit erzeugt oder verändert wurden und bis zum Stichtag der Analyse gelöscht und überschrieben wurden, stehen nicht mehr zur Verfügung. In



diesen Fällen können Minuten darüber entscheiden, wie erfolgreich eine Untersuchung verlaufen wird. Zeit ist also ein kritischer Faktor.

Die folgenden Untersuchungsobjekte werden in den meisten Analysen die Hauptrolle spielen:

- Betriebssystem
- Dateisystem
- VirensScanner und Personal Firewall
- Netzwerkprotokolle von Intrusion-Detection-Systemen
- Betriebssystemnahe Anwendungen
- Anwendungen
- Hauptspeicher

Die einzelnen Objekte werden von Betriebssystem zu Betriebssystem in anderer Form zu untersuchen sein. Dazu kommt, dass die meisten Objekte neben nichtflüchtigen Daten auch flüchtige Daten erzeugen. So enthält die Windows-Registry Daten, die von Benutzer zu Benutzer verschieden sein können, als auch Daten, die für alle Benutzer gleich sind. Dazu kommt, dass ein Teil der Einträge aus flüchtigen Daten bestehen, die beim Beenden des Betriebssystems verändert oder gelöscht werden. Die Ergebnisse einer Online-Analyse können also in vielen Fällen von den Ergebnissen einer Offline-Untersuchung abweichen.

13.6.4 Forensische Untersuchung

Ein Vorfall tritt ein. Die Meldung kann durch ein technisches System gegeben werden oder es handelt sich um einen Hinweis von einem Mitarbeiter oder um einen Polizisten mit einem Durchsuchungsbefehl in der Hand. Abhängig von der Schwere des Vorfalls und einigen anderen typischen betrieblichen Randbedingungen ist es unter Umständen nicht möglich, auf den Kollegen zu warten, der solcherart Untersuchungen normalerweise durchführt. In einem solchen Fall müssen Regeln existieren, die einer größeren Gruppe an Personen bekannt sind. Weitere Argumente für eine verbindliche Richtlinie zur Durchführung IT-forensischer Untersuchungen wurden in den letzten beiden Abschnitten aufgezählt: Eine im höchsten Maße formelle Vorgehensweise ist der einzige Garant dafür, dass die Ziele erreicht werden und die Ergebnisse im Nachhinein verwendet werden können.



KAPITEL 13 – MANAGEMENT VON SICHERHEITSEREIGNISSEN UND IT-FORENSIK

13

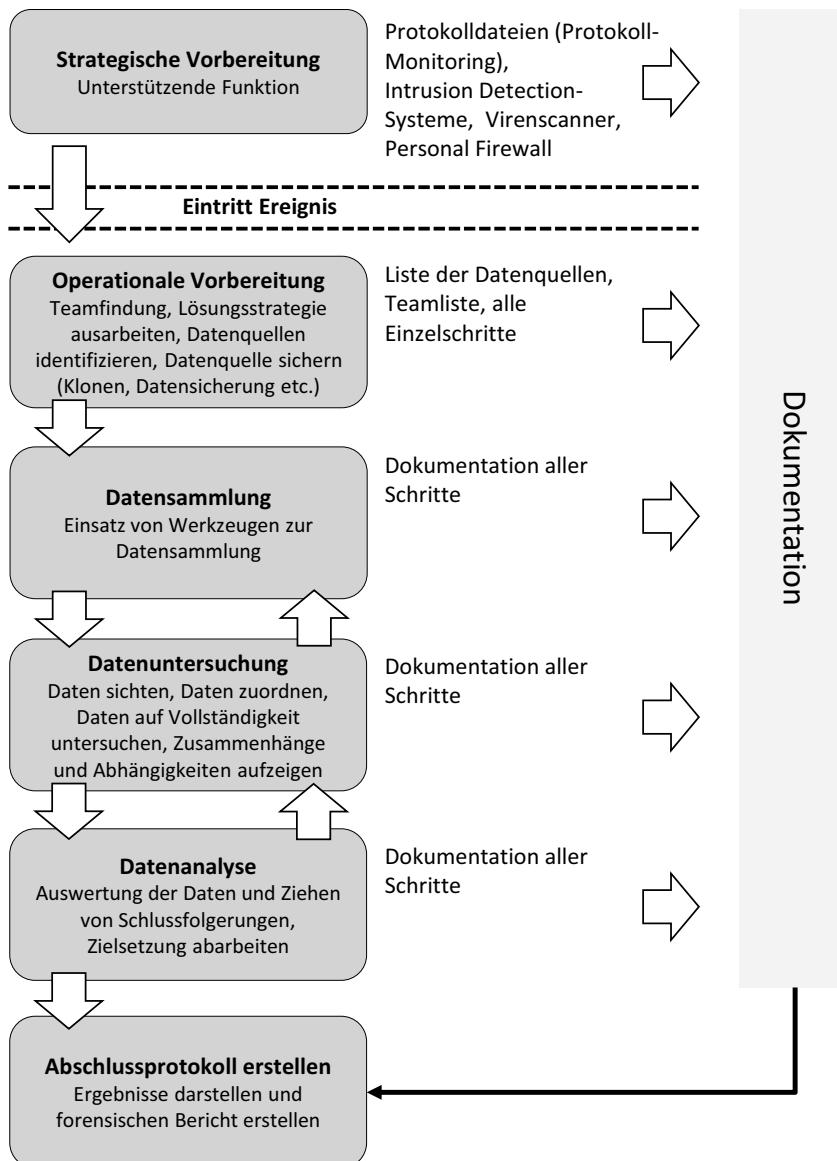


Abbildung 13.6: Einzelschritte der forensischen Untersuchung

Eine Richtlinie sollte die Vorgehensweise für alle Schritte der forensischen Untersuchung abdecken. Neben einer Beschreibung des Ablaufs einer vollständigen forensischen Untersuchung sollten folgende Punkte definiert werden:



- Die Voraussetzungen, dass eine Untersuchung vorgenommen werden darf, sollten genannt werden. Zusätzlich dazu sollte aufgezählt werden, welche Personen bzw. welche Rollen in jedem Fall Teil des Analyseteams sein müssen.
- Die rechtlichen Voraussetzungen, eine Analyse durchführen zu dürfen, ist stark vom Einzelfall abhängig. In einem Unternehmen gehören die Arbeitsmittel wie ein Rechner dem Unternehmen und können deshalb leichter in Zugriff genommen werden als private, vom Mitarbeiter mitgebrachte Gerätschaften. Aber auch im Falle von IT-Systemen des Unternehmens sollten Vorgaben existieren, wie mit personenbezogenen Informationen umgegangen werden muss.
- Die Anforderungen an die Qualität der Methoden und eine Bestimmung der Begriffe.

Die Vorgehensweise bei der Durchführung einer forensischen Untersuchung ist gesetzlich nicht vorgeschrieben. Auch hier macht es aber Sinn, den Empfehlungen (*best practices*) von Standards und damit befassten Institutionen zu folgen. In Abbildung 13.6 wird eine Schrittfolge aufgezeigt, die sich in den letzten Jahren bewährt hat und die in dieser Form im Dokument »Leitfaden IT-Forensik« des BSI aufgezeigt wird. Das BSI greift in diesem Fall wiederum auf Quellen anderer Institutionen zurück.

Die strategische Vorbereitung

Im Rahmen der Vorbereitungsphase werden bereits Maßnahmen implementiert, die eine eventuell später stattfindende Untersuchung unterstützen können. Dazu gehören die Aktivierung von Protokoldiensten und die Einführung von Werkzeugen zum Protokoll-Monitoring. Zur strategischen Vorbereitung gehört auch die Implementierung von Werkzeugen im Netzwerkbereich wie ein Intrusion-Detection-System (IDS) oder die Ausbringung von Honeypots.

Die operationale Vorbereitung

Ein Vorfall ist eingetreten. Bevor nun das Team anfängt, eine Analyse zu starten, sollte zunächst die Zeit gefunden werden, im Vorfeld der Analyse eine Bestandsaufnahme durchzuführen. Dazu gehört die Beantwortung der Fragen, ob alle erforderlichen Personen bzw. Rollen anwesend sind, ob alle Vorekehrungen getroffen wurden, die Anforderungen an die Untersuchung erfüllen zu



können, und ob alle potenziellen Quellen für Daten, die später analysiert werden sollen, identifiziert wurden.

Die Datensammlung

In diesem Abschnitt wird vorgegeben, wie die technische Vorgehensweise aussehen muss, wenn es darum geht, Daten sicherzustellen. Dazu gehört z.B. die Anfertigung von Images und Backups. Mit technischen und organisatorischen Mitteln muss sichergestellt werden, dass die Ursprungsdaten, falls möglich, ungefährdet gesichert abgelegt werden. Dazu können Festplatten ausgebaut und in versiegelte Behälter verbracht werden. In Fällen, in denen eine Analyse von Speicherbereichen oder Netzwerkaktivitäten erforderlich wird, ist es umso wichtiger, alle Zugriffe zu protokollieren, und dies in möglichst revisionssicherer Weise.

13

Datenuntersuchung

Zu diesem Zeitpunkt liegt eine Menge an Informationen vor, die direkt oder indirekt mit dem Ereignis zu tun haben. Die Daten bestehen aus Dateien, Fragmenten von Datenpaketen, Screenshots von Konfigurationen und Aufschrieben, die zum Teil bereits Vermutungen beinhalten. Nun muss diese Datensammlung sortiert und priorisiert werden. Zunächst muss die Entscheidung getroffen werden, ob alle Spuren ausreichend genau verfolgt wurden oder ob nicht der Schritt Datensammlung erneut gestartet werden muss, z.B. mit einem veränderten Zielobjekt wie einem weiteren Rechner oder einer neuen Anwendung.

Die eigentliche Analyse der Daten

In den meisten Fällen wird eine Untersuchung anhand von Protokolldaten und Dateien im Dateisystem stattfinden. Für weitergehende forensische Ermittlungen wie die Interpretation des Hauptspeichers werden den allermeisten Firmen das Know-how und die erforderlichen Mittel fehlen. Handelt es sich um Protokolldateien, dann ist darauf zu achten, dass nicht nur der Inhalt der Dateien wichtig ist, sondern auch alle weiteren Zusammenhänge, die eine der Zielsetzungen beantworten könnten. Dazu gehört das Erstellungsdatum, der Urheber, der Speicherort, die Struktur oder der Zusammenhang mit weiteren Protokolldateien oder anderen Dateien.



Die Dokumentation

Die umfassende und vollständige Dokumentation enthält zum einen die Einzelereignisse der Vorbereitung und der Untersuchung und zum anderen die Ergebnisse. Aus diesem Grund unterteilt man diese in den Prozess begleitenden Teil und den Teil der abschließenden Dokumentation.





14 Kennzahlen

14.1 Kapitelzusammenfassung

Dinge messbar und damit vergleichbar und besser darstellbar zu machen, ist grundsätzlich eine wichtige Anforderung in einem Unternehmen. Das gilt auch für das eher abstrakte Thema IT-Security. Wie sicher ist ein Unternehmen? Wie gut ist der Schutz besonders kritischer Informationen? Wie hoch ist der Grad an Wirksamkeit der Maßnahmen, die dem Schutz personenbezogener Daten dienen? Diese Fragen treffen regelmäßig auf ein Gebiet, das in hohem Maße mit Wahrscheinlichkeiten arbeitet und von mangelhafter Transparenz gekennzeichnet ist.

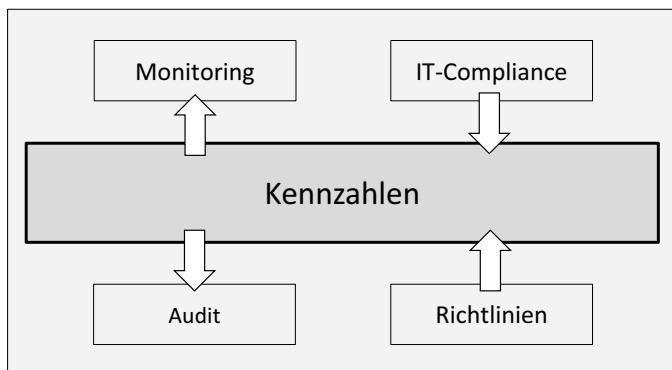


Abbildung 14.1: Primäre Abhängigkeiten von anderen Themen der IT-Security

Die Entwicklung und Berechnung von Kennzahlen stellt das Werkzeug dar, das dem Manager IT-Security die Möglichkeit geben soll, von ungewissen Annahmen zu verlässlichem Wissen zu gelangen. Was Kennzahlen auszeichnet, wie sie definiert werden und wie eine Berechnung aussehen kann, wird im aktuellen Kapitel erläutert. Eine Methodik, strukturiert mit Kennzahlen zu arbeiten, ist der Einsatz im Rahmen einer Balanced Scorecard. Wie eine solche definiert werden kann, wird zum Ende des Kapitels geschildert.



Die Top-3-Fragen zum aktuellen Kapitel:

- Existiert eine Liste mit IT-Security-Kennzahlen und werden diese regelmäßig berechnet?
- Werden IT-Security-Kennzahlen im Rahmen des IT-Risikomanagements genutzt, um die Wirksamkeit von Maßnahmen zu überprüfen?
- Sind Automatismen implementiert, um Kennzahlen zu berechnen? Ist ein vorhandenes SIEM in die Berechnung von Kennzahlen eingebunden?

14.2 Einführung

14

Um die Wirksamkeit von Maßnahmen beurteilen zu können, muss der Zustand der IT-Security zu verschiedenen Zeitpunkten messbar gemacht werden. Dabei werden einige Anforderungen an die Messungen gestellt, denn schließlich muss die Messung nachvollziehbar und zudem noch am besten über jeden Zweifel und jede Interpretation erhaben sein. Jeder Mathematiker weiß natürlich, dass die Wahl der Messmethode entscheidenden Einfluss auf das Ergebnis hat, und in der IT-Security sieht es nicht anders aus. Mit der Entscheidung, was gemessen werden soll und an welcher Stelle, wird auch über die Qualität des Ergebnisses entschieden. Desto wichtiger ist es, sich bei der Wahl und dem Einsatz von Kennzahlen einige Gedanken zu machen.

14.3 Die Aufgabe von Kennzahlen

Das IT-Risikomanagement beschreibt, wie Risiken für den Geschäftsbetrieb erfasst werden und wie diese auf Basis der Klassifizierung nach Wichtigkeit sortiert werden können. Diese Arbeit ist wichtig und bildet das Rückgrat der IT-Security. Dennoch ist es entscheidend, darüber nicht den Blick auf das Gesamtbild zu verlieren. Der Einbezug von Experten, z.B. in Form des Data Owners, für die Bewertung von Sachverhalten ist wichtig, damit nicht die falschen Systeme und Daten überbewertet werden. Trotzdem stellen sie nur eine Meinung dar. Um dieser Meinung etwas Messbares zur Seite zu stellen, gewinnt der Bereich der »Metrics«, auf Deutsch »Kennzahlen«, eine immer größere Wichtigkeit.



Hinweis

Wenn in der ISO 27001 von »Maßen« die Rede ist, mit denen die erfolgreiche Umsetzung von Maßnahmen überprüft werden soll, sind die hier behandelten Kennzahlen gemeint.

Eine weitere Aufgabe von Kennzahlen ist es, die Gefahr durch Bedrohungen qualitativ und quantitativ zu bewerten. Dadurch soll gewährleistet werden, dass das oftmals schmale Budget schwerpunktmäßig für die Abwehr der wirklich drängenden Gefahren aufgewandt wird und nicht für nur vermeintlich als wichtig eingestufte Bedrohungen. Das umfasst alle Arten der Lenkung von Entscheidungsprozessen in der IT-Security durch die Ergebnisse von Kennzahlen.

Zusammengefasst kann man sagen, dass Kennzahlen der Quantifizierung der IT-Security dienen. Sie haben die Aufgabe, das sehr schwer fassbare Gebiet von Bedrohungen und deren Abwehr durch Zahlenmaterial bewertbar und vergleichbar zu machen. Möchte man z.B. Risiken miteinander verglichen oder aber den Zustand vor und nach der Einführung einer Maßnahme darstellen, so sind Kennzahlen sehr nützlich. Auf der anderen Seite bilden auch Kennzahlen nicht die exakte Wirklichkeit ab und sind nur ein weiterer Weg der Annäherung an eine möglichst objektive Einschätzung.

Der maßgebliche Grund für die Einführung von IT-Security-Kennzahlen ist, dass sie eine der verlässlichsten Möglichkeiten ist, von Entscheidungen nach Bauchgefühl hin zu einem mit Fakten unterlegten IT-Risikomanagement zu gelangen. Für die Unternehmensleitung bis hinunter zum Manager IT-Security dienen Kennzahlen der Herstellung von Transparenz und vermögen es, nebulöse Annahmen in Zahlenmaterial zu verwandeln. Das unterstützt z.B. ganz maßgeblich die von außen herangetragene Forderung, konkret die Einsparungen nachzuweisen, die die IT-Security erbringt.

IT-Security-Kennzahlen haben somit die folgenden Aufgaben:

- Sie machen IT-Risikomanagement und damit die IT-Security messbar und dadurch transparent und vergleichbar.
- Sie machen den Umsetzungsgrad von Maßnahmen messbar.
- Sie machen die Wirksamkeit von Maßnahmen messbar.



KAPITEL 14 – KENNZAHLEN

- 14
- Sie ermöglichen Entscheidungen auf Basis von »nachher-vorher« und »Was passiert, wenn«-Analysen.
 - Sie bilden das Fundament für Investitionsentscheidungen, da sie deutlich machen, an welchen Stellen sich Investitionen lohnen und an welchen nicht.
 - Sie zeigen Kosteneinsparungen auf, also den *Return on Security Investment* (ROSI).

IT-Security ist einer der wenigen Bereiche innerhalb von Unternehmen, für die es kaum übergreifend bekannte und auch anerkannte Kennzahlen gibt. In Bereichen wie dem Finanzcontrolling oder dem Einkauf ist dies anders. Die dort verwendeten Instrumentarien sind seit vielen Jahrzehnten bekannt. Die Folge daraus ist, dass maßgeschneiderte IT-Security-Kennzahlen nicht für jede Branche und für jedes Unternehmen zur Verfügung stehen. Das führt zu zwei Problemen. Der Manager IT-Security kann gezwungen sein, eigene Kennzahlen und die zur Erfassung gehörende Methodik festzulegen. Dadurch kommt es zum zweiten Problem. Kennzahlen werden dadurch nicht immer vergleichbar sein. Um diesem Problem vorzubeugen, bilden sich zurzeit Interessengruppen mit dem Ziel, Kennzahlen zu sammeln und wenn möglich zu verallgemeinern.

Im Rahmen von ITIL (IT Infrastructure Library), einer Sammlung von Best-Practice-Dokumenten zur Unterstützung des Aufbaus eines IT-Service-Managements, werden unter den »Key Performance Indicators« oder KPIs auch IT-Security-Kennzahlen geführt. Im Rahmen der Dokumente zum IT-Security-Management sind dort einige Kennzahlen zusammengetragen worden, die einen ersten wichtigen Schritt darstellen. Dazu gehören Downtime-Zeiten von IT-Systemen, die Anzahl an erfassten Sicherheitsvorfällen, Statistiken von IT-Security-Schulungen oder die Messung von Prozessen wie z.B. die Umsetzung von Maßnahmen nach Bekanntwerden eines Sicherheitslochs.

Im Rahmen der ISO-2700x-Reihe wird das Thema in der Norm ISO 27004 »Information technology – Security techniques – Information security Management – Measurement« wieder aufgegriffen. Auch in diesem Dokument zeigt sich die Schwierigkeit, konkrete Kennzahlen zu definieren. Aus diesem Grund konzentriert man sich im Wesentlichen auf die wichtigen Schritte, die unternommen werden müssen, um eine Kennzahlenmethodik einzuführen:



- eine Einführung in das Messen von IT-Security
 - Darstellung der Verantwortung der Unternehmensführung
 - die Planung, welche Kennzahlen zu welchem Zweck erfasst und ausgewertet werden sollen, wer dafür verantwortlich ist und in welchem Zeitabständen dies zu erfolgen hat
 - die Entwicklung von eigenen Kennzahlen
 - das Arbeiten mit Kennzahlen
 - die Vorgehensweise bei der Analyse von Messdaten, deren Auswertung und Darstellung
 - Hilfestellungen zur Überprüfung und Weiterentwicklung von Kennzahlen

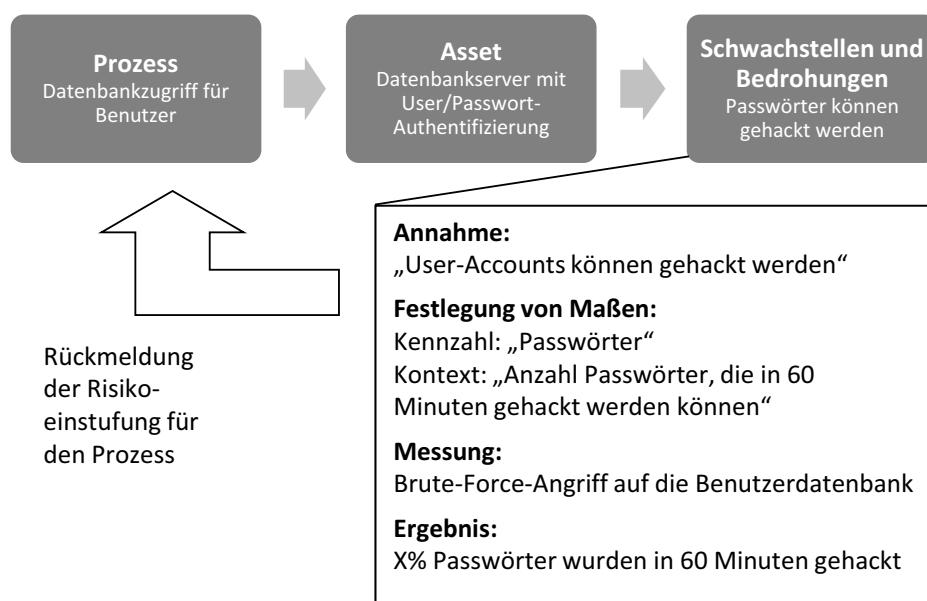


Abbildung 14.2: Kennzahlen im IT-Risikomanagement-Prozess

In den Anhängen zur ISO 27004 finden sich Beispiele für Kennzahlen.

14.4 Quantifizierbare Kennzahlen

Kennzahlen, die ihre Aufgabe erfüllen sollen, müssen so weit wie möglich in Zahlen ausgedrückt werden können. Also genau das Gegenteil von ungenau



spezifizierten Ampeln oder Smileys. Je mehr Auswertungen man auf Basis von Prozenten oder ganzen Zahlen präsentieren kann, desto glaubhafter wird der Bericht sein. Investitionsentscheidungen werden im Allgemeinen leichter getroffen, wenn dargestellt werden kann, dass 85 % aller Malware vermieden werden kann, wenn ein spezielles Produkt eingesetzt wird, als wenn man seinen Antrag mit einem »Daumen-hoch-Symbol« versieht. Natürlich ist dies nicht in jedem Fall möglich, und die Einschätzung eines Risikos wird zumeist nicht mit genauen Prozentangaben zu belegen sein. Aus diesem Grund gibt es einige Modelle, um diesem Problem entgegenzuwirken. Eines davon ist der NPLF-Ansatz, der in der ISO 15504 beschrieben wird. »NPLF« steht in diesem Fall für »Not, Partially, Largely, Fully« und bezeichnet vier Stadien, nach denen Fragestellungen eingeordnet werden können.

14

Die Zahlen, die dahinterstecken, sind folgendermaßen definiert:

- Nicht erreicht (*not achieved*), dargestellt mit roter Farbe: 0–15 % Umsetzungsgrad
- Teilweise erreicht (*partially achieved*), dargestellt mit gelber Farbe: 16–50 % Umsetzungsgrad
- Weitgehend erreicht (*largely achieved*), dargestellt mit hellgrüner Farbe: 51–85 % Umsetzungsgrad
- Vollständig erreicht (*fully achieved*), dargestellt mit dunkelgrüner Farbe: 86–100 % Umsetzungsgrad

Dieser Ansatz bietet nicht das gesamte Spektrum ganzer Zahlen zwischen 1 und 100, sondern für jede Stufe einen Zahlenbereich, der im nächsten Verarbeitungsschritt wieder auf jeweils eine Zahl umgeschlagen werden muss. Im Grunde handelt es sich also um verbesserte Ampeln, deren Wertebereich zumindest definiert ist. Dadurch gewinnen die Kennzahlen an Vergleichbarkeit und damit auch an Akzeptanz.

Die ISO 15505, in vielen Branchen auch als Norm, in der SPICE thematisiert wird (Software Process Improvement and Capability Determination), zeigt Wege auf, um Fortschritte in Prozessen zu erfassen und aufzuzeigen. Der vollständige Titel der Norm lautet dementsprechend »Information technology – Software process assessment«.

Natürlich ist die Darstellung von Fortschritten mittels des NPLF-Ansatzes nur eine Möglichkeit, unscharfe oder schwammige Einstufungen einzustufen.



und mit Zahlen zu hinterlegen. Auch in diesem Fall wird eine Einordnung z.B. nach »teilweise erreicht« nur eine Bandbreite von 16–50 % Umsetzungsgrad ergeben, und es stellt sich nun wieder die Frage, ob der Mittelwert für Berechnungen herangezogen werden sollte oder vielleicht einer der beiden Werte, also 16 % oder 50 %. Die Entscheidung darüber hängt in großem Maße davon ab, für welche Art Berechnung diese Zahlen im Nachhinein herangezogen werden sollen.

14.5 Steuerung mithilfe von Kennzahlen

Ohne Frage stellt das Patchmanagement für Computer, Server und natürlich ebenso für aktive Netzwerkkomponenten ein wichtiges Arbeitsgebiet in der IT-Security dar. Das Gleiche gilt auch für die Aktualisierung jedes einzelnen Softwareprodukts auf jedem Rechner, das jeweils auf dem neuesten Stand gehalten werden muss. Wird das reine Betriebssystem noch in den meisten Firmen halbwegs aktuell gehalten, so gilt dies schon für die Software, die darauf installiert ist, nur noch bedingt. Es gib Studien, die eine Rechnung aufstellen, die folgendermaßen aussieht: Unternehmen mit 10.000 Benutzern nutzen ca. 600–800 verschiedene Softwareprodukte auf Arbeitsplatzrechnern. Bei 25.000 Benutzern gehen die Zahlen bereits in den vierstelligen Bereich. Die wirklich akkurate Pflege einer derart großen Anzahl von Softwareprodukten bedingt große Ressourcen. Die Frage, ob es sich aus Sicht einer Kostenabwägung wirklich lohnt, diesen Schutz aufrechtzuerhalten, ist demnach sicherlich angebracht. Eine naheliegende Alternative zur Softwareaktualisierung wäre, den Passwortschutz durch eine Zwei-Faktor-Authentifizierung zu ergänzen, z.B. durch Hardware-Token zusätzlich zum Passwort, und den Virenschutz auf den Servern und Arbeitsplatzrechnern durch ein zweites Antivirenprodukt zu verbessern. Eine Policy, die jede Speicherung von Daten auf dem lokalen Rechner verbietet und das Verhindern von lokal gespeicherten temporären Dateien sowie der Überschreibschutz von Daten im Netzwerk wären zusätzlich erforderlich. Sind diese alternativen Maßnahmen umgesetzt, dann könnte der lokale Schutz der PCs vollständig aufgegeben werden.

Dieses Beispiel soll zeigen, dass selbst eine gut überlegte und traditionell als wichtig erachtete Maßnahme, in diesem Fall ein halbherziges Patchmanagement (sprich die Konzentration auf Betriebssystem und einige Applikationen) nicht immer auch die logische Vorgehensweise darstellen muss. IT-Security-



KAPITEL 14 – KENNZAHLEN

Management bedeutet in diesem Fall, Kennzahlen zu nutzen, Methoden zu überprüfen und gegen alternative Vorgehensweisen zu vergleichen. Die Kosten für die beiden möglichen Wege stellen eine erste Kennzahl dar. Um den jeweiligen Grad an Sicherheit beurteilen zu können, müssten zudem die bislang aufgetretenen Sicherheitsvorfälle erfasst werden. Die Beurteilung, wie viele dieser Vorfälle durch die eine oder andere Methodik verhindert worden wären, ist dann wieder eine Aufgabe eines Experten und liefert schlussendlich eine Bewertung, die den jeweiligen Kosten entgegengestellt werden kann.

Das Beschreiten ungewöhnlicher Wege führt auch in der IT-Security oft zu Unverständnis. Selbst in dieser doch recht neuen Disziplin haben sich bestimmte Wertvorstellungen und Arbeitsweisen durchgesetzt und werden nicht selten durch die Softwareindustrie zementiert. Davon abzuweichen, bedeutet deshalb häufig, ein persönliches Risiko einzugehen. Es liegt also nahe, Kennzahlen zu nutzen, um Entscheidungen auf konkrete Zahlen zu stützen. Daraus folgt, dass Manager IT-Security auf Basis von Kennzahlen ermitteln können, wie sie ihre Zeit und ihr Budget am sinnvollsten verwenden sollten. Oft stellt sich dabei heraus, dass Sicherheitslöcher, die bis dato kaum Beachtung gefunden haben, eine deutlich höhere Bedrohung darstellen. So zeigen aktuelle Berechnungen, dass der Bereich der Awareness deshalb an Bedeutung gewinnen sollte, weil viele sehr teure Sicherheitsvorfälle aufgrund von menschlichen Fehlern geschehen und durch bessere Aufklärung zu einem hohen Prozentteil verhindert werden könnten. Oft macht es also mehr Sinn, 10.000 € in eine Aufklärungskampagne zu investieren, als 50.000 € in eine Software, die im Nachhinein Fehler ausbessern soll.

Ein weiteres Feld, in dem Kennzahlen eine große Rolle spielen, ist die Steuerung und Kontrolle der Umsetzung von Sicherheitsmaßnahmen, die durch Systeme zur Erfassung von Sicherheitsereignissen erfasst werden. Ein entsprechend aufgestelltes SIEM kann z.B. die Anzahl an veralteten, auf den Arbeitsrechnern installierten Office-Installationen erfassen. Ist der prozentuale Anteil größer als eine zuvor festgelegte Menge an Rechnern, dann kann ein Ticket erzeugt werden, diesen Missstand zu beheben. Ähnlich gelagert sind Kennzahlen, die den Zeitraum von der Ermittlung eines kritischen Sicherheitsvorfalls bis zu dessen Behebung erfassen und dokumentieren. Ist die Zeitdauer zu lang, dann muss dies ersichtlich werden, um entsprechende Maßnahmen festlegen und umsetzen zu können.



14.6 Qualität von Kennzahlen

Gute Statistiken sind diejenigen, die man selbst erzeugt, denn sie lassen sich auch am besten manipulieren.

Man ist schnell geneigt, einer Statistik zu glauben. Klare Zahlen und eine schöne Aufmachung sind die halbe Miete. Das führt dazu, dass immer mehr vollkommen unsinnige Kennzahlen aufgebracht und verbreitet werden. Wenn es um die Erreichung eines Sicherheitslevels geht, ist es deshalb entscheidend, dass der gesamte Prozess von der Definition sinnvoller Kennzahlen bis hin zur korrekten Auswertung und letztendlich Darstellung von einer hohen Qualität gekennzeichnet ist.

14.6.1 Gute Kennzahlen

14

Vor der Auswertung und Präsentation von Kennzahlen steht der Prozess, zu ermitteln, welche Kennzahlen Verwendung finden und für welche Zwecke sie genutzt werden sollen. Naturgemäß hängt von dieser Entscheidung die Qualität der Ergebnisse ab, und sie sollte damit nicht leichtfertig getroffen werden. Dazu kommt, dass der Prozess, Kennzahlen mit Zahlenmaterial zu unterfüttern, aufwendig ist und einige Zeit in Anspruch nehmen kann.

Gute Kennzahlen erkennen Sie an folgenden Eigenschaften:

- Gute Kennzahlen sind einfach zu ermitteln. Idealerweise werden sie automatisiert erfasst und verarbeitet.
- Gute Kennzahlen bestehen aus ganzen Zahlen, Prozentangaben oder zumindest aus definierten Abstufungen in Ampelmodellen. Farben werden konkreten Umsetzungsgraden in Prozentangaben zugeordnet.
- Gute Kennzahlen beziehen sich auf ein Maß wie z.B. Zeit- oder Währungseinheiten.
- Gute Kennzahlen sprechen für sich selbst. Aus der Angabe »mittellange Downtime« wird ein Budgetverantwortlicher kaum Rückschlüsse auf eine Neuinvestition ziehen können.
- Gute Kennzahlen spiegeln die reale Welt so objektiv wie möglich wider. Dies ist einfach zu überprüfen, indem man die gleichen Fragen verschiedenen Personen vorlegt. Unterscheiden sich die Antworten, also die Kenn-



zahlen, von Person zu Person, dann sollte man darüber nachdenken, andere Kennzahlen zu suchen.

- Gute Kennzahlen sind unternehmens- und organisationsunabhängig. Durch ist es möglich, zwischen Abteilungen und auch Unternehmen zu vergleichen und das eigene Unternehmen gegen unabhängige externe Statistiken zu vergleichen (*company benchmark*).

14.6.2 Schlechte Kennzahlen

Nachdem die Kriterien für gute Kennzahlen vorgestellt wurden, sollen nun auch die schlechten Kennzahlen in den Fokus rücken. Schlechte Kennzahlen sind unspezifisch, passen nicht zum eigenen Unternehmen, spiegeln nicht die Wichtigkeit der verschiedenen, überwachten Prozesse wider, sind teuer in der Erfassung, z.B. ausschließlich über spezielle Hard- und Software umsetzbar, oder sind der subjektiven Meinung einer Person unterworfen.

Leider sind viele Kennzahlen, die direkt auf Normen basieren, schlechte Kennzahlen, weil versucht wird, allgemeine Standardempfehlungen in individuelle Kennzahlen zu transformieren, ohne die oben aufgeführten Kriterien für gute Kennzahlen zu beachten.

14.6.3 Vergleichbarkeit von Kennzahlen

Kennzahlen dienen in den meisten Fällen entweder der Rechtfertigung von Ausgaben oder der Nachverfolgung der Effektivität von Maßnahmen. Sie haben damit die Aufgabe, ein schwer zu überblickendes Aufgabengebiet transparenter zu machen. Dies kann gut gelingen, solange die verwendeten Kennzahlen alle Kriterien erfüllen, die sie zu guten Kennzahlen machen, und dazu gehört vor allem, dass sie einer Überprüfung durch Dritte standhalten.

Eine große Herausforderung an die Identifizierung von Kennzahlen liegt darin begründet, dass es kaum allgemein gültige und allgemein anerkannte Kennzahlen im Bereich der IT-Security gibt. Damit sind auch die Vergleichbarkeit und der damit verbundene Erkenntnisgewinn nur eingeschränkt vorhanden. Die ISO 27004 geht einen ersten Schritt in die richtige Richtung, indem sie zumindest den Prozess zur Ermittlung von Kennzahlen skizziert und bereits einige Beispiele nennt.



Große Unternehmensberatungen tauschen ihre Kennzahlen untereinander aus, um Branchenvergleiche anstellen und in Form von Benchmark-Tabellen darstellen zu können. Die völlig natürliche Frage der Unternehmensleitung, »Wo stehen wir denn bezüglich der IT-Security im Vergleich zu anderen Unternehmen?«, kann durch solche Darstellungen zumindest ansatzweise beantwortet werden.

Für das eigene IT-Security-Management bedeutet dies, dass in erster Linie Kennzahlen verwendet werden sollten, die die Kriterien für gute Kennzahlen erfüllen. Im zweiten Schritt sollte auch immer ein Auge darauf geworfen werden, welche Berechnungsmethoden in den einschlägigen Standards angeboten werden. Zudem sind zahlreiche Diskussionsgruppen im Internet aktiv, die sich vorrangig mit der Problematik der Findung und Nutzung geeigneter Kennzahlen beschäftigen.

14

14.7 Verschiedene Kennzahlen aus der IT-Security

In der nachfolgenden Tabelle sind einige Beispiele für Kennzahlen aufgeführt. Die Kapitelangabe in der ersten Spalte bezieht sich auf den Anhang A der ISO 27001, der in diesem Fall zur Orientierung und Einordnung dient. Wie bereits erwähnt, basieren gute Kennzahlen auf harten, nachweisbaren Zahlen. Vorgaben aus Richtlinien sind dahin gehend aber eher schwammig, und es müssen daher für jede Vorgabe eine oder auch mehrere passende Kennzahlen entwickelt werden. In vielen Fällen wirken verschiedene Kennzahlen zusammen und haben erst zusammengenommen die gewünschte Aussagekraft.

Bereich	Hintergrund	Kennzahl
Leitlinie zur Informations-sicherheit	Eine Reihe von Basisrichtlinien bildet das Grundgerüst des IT-Security-Managements. Dazu gehören unter anderen die Sicherheitsrichtlinie und die Klassifizierungsrichtlinie.	Umsetzungsgrad (in %) der Basisrichtlinien



KAPITEL 14 – KENNZAHLEN

14

Bereich	Hintergrund	Kennzahl
	Insbesondere die Basisrichtlinien müssen zwingend unternehmensweit verbindlich und bekannt sein. Dafür kann es erforderlich sein, diese Richtlinien in jedem Tochterunternehmen einzeln verbindlich zu machen. Dies kann durch Aushang, persönlicher Unterschrift jedes Mitarbeiters oder anderer Maßnahmen geschehen.	Anteil (in %) der Mitarbeiter, die an einer Schulung zu den Basisrichtlinien teilgenommen haben Anteil (in %) der Mitarbeiter, die durch Unterschrift die Verbindlichkeit der Basisrichtlinien anerkannt haben
Interne Organisation	Es soll gemessen werden, in welchem Umfang eine Unterstützung der IT-Security durch das Management vorhanden ist. Der Fokus liegt dabei auf der Umsetzung von Maßnahmen und der Implementierung von Prozessen. Grundlage sind die entsprechenden Dokumente aus dem ISMS, auf denen die verantwortlichen Mitarbeiter dokumentiert sind.	[Gesamtzahl aller Maßnahmen, die von der Unternehmensleitung ausdrücklich unterstützt werden] geteilt durch die [Gesamtzahl aller Maßnahmen]
Externe Organisation	Externe Unternehmen mit Zugangsrechten und Zugriffsrechten auf Unternehmensdaten müssen definierten Sicherheitsstandards genügen.	[Gesamtzahl aller externen Unternehmen, die auf die Einhaltung der Sicherheitsstandards überprüft wurden] geteilt durch die [Gesamtanzahl aller externen Unternehmen mit Zugriffsrechten auf Unternehmenswerte]



VERSCHIEDENE KENNZAHLEN AUS DER IT-SECURITY

Bereich	Hintergrund	Kennzahl
Verantwortung für Unternehmenswerte	Werte müssen identifiziert und inventarisiert werden, um anhand dieser Inventarliste geeignete Maßnahmen definieren und überprüfen zu können. Die Anzahl aller Werte kann bei IT-Systemen häufig elektronisch ermittelt werden.	[Anzahl inventarisierte und beschriebene Werte] geteilt durch [Gesamtanzahl Werte]
Klassifizierung von Informationen	Werte müssen auf Basis der Klassifizierungsrichtlinie klassifiziert werden.	[Anzahl klassifizierte Werte] geteilt durch [Gesamtanzahl Werte]
Personalsicherheit vor der Einstellung	Bevor ein neuer Mitarbeiter Zugriff auf Unternehmenswerte erhält, sollte eine Schulung stattfinden, in der die Unternehmensrichtlinien im Umgang mit Equipment oder Daten erläutert werden.	[Anzahl durchgeführter Schulungen vor Erteilung von Zugriffsberechtigungen pro Zeiteinheit] geteilt durch [Gesamtanzahl neuer Mitarbeiter pro Zeiteinheit]
Personalsicherheit während der Einstellung	Regelmäßig durchgeführte Schulungsmaßnahmen halten die Mitarbeiter über aktuelle Themen der IT-Security auf dem Laufenden.	[Anzahl Mitarbeiter, die regelmäßig an Schulungsmaßnahmen teilnehmen] geteilt durch [Gesamtanzahl Mitarbeiter]
	Mitarbeiter, die in sensiblen Bereichen arbeiten bzw. Zugriff auf hoch klassifizierte Daten haben, sollten mittels Background-Check überprüft werden. Dazu gehören insbesondere auch Administratoren von IT-Systemen.	[Anzahl durchgeführter Background-Checks] geteilt durch [Gesamtanzahl in sensiblen Bereichen tätige Mitarbeiter]



KAPITEL 14 – KENNZAHLEN

14

Bereich	Hintergrund	Kennzahl
Personalsicherheit bei Beendigung oder Änderung der Anstellung	Wenn ein Mitarbeiter das Unternehmen verlässt, muss sichergestellt werden, dass alle Zugriffsrechte zeitnah angepasst werden.	[Anzahl ausgeschiedener Mitarbeiter, denen alle relevanten Zugriffsrechte entzogen wurden] geteilt durch [Gesamtanzahl ausgeschiedene Mitarbeiter] [Anzahl Personen, deren Ausscheiden der IT-Abteilung gemeldet wurde] geteilt durch [Anzahl ausgeschiedene Personen]
Sicherheitsbereiche	Der Zutritt zu Büroräumen, Rechenzentren und anderen sensiblen Bereichen muss kontrolliert erfolgen. Im ersten Schritt werden dafür diese Bereiche identifiziert und klassifiziert. Im zweiten Schritt werden auf Basis der Klassifizierung die entsprechenden Maßnahmen umgesetzt.	Anteil (in %) der sensiblen Bereiche, die durch spezielle Zugangsregeln geschützt sind
Verfahren und Verantwortlichkeiten	Der Zugang zu IT-Systemen mit sehr hoher Klassifizierung kann unter anderem durch die Implementierung spezieller Zugangsverfahren kontrolliert werden, z.B. durch die Implementierung des Vieraugenprinzips.	[Anzahl IT-Systeme mit hochsicherem Zugangsverfahren] geteilt durch [Gesamtzahl sehr hoch klassifizierter IT- Systeme]
Management der Dienstleistungserbringung durch Dritte	Externe Dienstleister sollten regelmäßig darauf überprüft werden, ob die einmal vergebenen Zugriffsrechte auch weiterhin benötigt werden.	[Anzahl der überprüften externen Dienstleister] geteilt durch [Gesamtanzahl externe Dienstleister mit Zugriffsrechten]



VERSCHIEDENE KENNZAHLEN AUS DER IT-SECURITY

Bereich	Hintergrund	Kennzahl
Schutz vor Schadsoftware	PCs, auf denen die erforderlichen Patches nicht eingespielt wurden, gefährden den Schutz der Daten und die Verfügbarkeit der IT-Infrastruktur.	(In %) Anteil der Arbeitsplatzrechner mit vollständigen Betriebssystempatches (In %) Anteil der PCs mit vollständigen Software-patches (In %) Anteil vollständiger aktueller Softwareprodukte an der Gesamtzahl der installierten Softwareprodukte
	Bestimmte offene Netzwerkports oder veraltete Netzwerkprotokolle können es Schadsoftware ermöglichen, auf das Betriebssystem oder auf installierte Software zuzugreifen. Die Erfassung kann unter Zuhilfenahme von Netzwerk-Scannern erfolgen.	(In Zahlen) Anzahl an Rechnern, die über definierte Protokolle (z.B. SMB1 – siehe WannaCry) angreifbar sind. (in Zahlen) Anzahl an Rechnern, auf denen angreifbare Software installiert ist, die auf bekannten Netzwerk-Ports basieren (z.B. FTP).
Backup	Backup-Medien müssen in einem vom Originalspeicher getrennten Brandabschnitt aufbewahrt werden. Unternehmenskritische Daten sollten zudem katastrophensicher aufbewahrt werden.	[Anzahl von Speichermedien, die katastrophensicher gelagert werden] geteilt durch [Gesamtanzahl aller Speichermedien] [Datenverlust in Stunden bei einem Brand an einem Montagabend, Dienstagabend, ...]
	Konfigurationsdaten müssen regelmäßig, wenn nicht bei jeder Änderung, gesichert werden. Dazu gehören vor allem auch die Konfigurationsdaten von aktiven Netzwerkkomponenten.	[Anzahl aktueller Sicherungen von Konfigurationen aktiver Netzwerkkomponenten] geteilt durch [Anzahl aller aktiven Netzwerkkomponenten]



Bereich	Hintergrund	Kennzahl
Anforderungen an die Zugangs-kontrolle	Externe Dienstleister sollen regelmäßig darauf überprüft werden, ob die vergebenen Zugangsrechte auch weiterhin benötigt werden.	[Anzahl der Dienstleister, deren Zugangsrechte überprüft wurden] geteilt durch [Gesamtanzahl externe Dienstleister mit Zugangs-rechten]
Benutzer-verwaltung	Bestehende Benutzerkonten sollen regelmäßig daraufhin überprüft werden, ob die dazugehörigen Benutzer noch aktuell sind und ob die zugewiesenen Rechte noch benötigt werden.	[Anzahl überprüfter Benutzerkonten] geteilt durch [Gesamtanzahl Benutzerkonten]
Verantwortung der Benutzer	Die Qualität von Passwörtern ist ein wichtiger Indikator für die Datensicherheit. Diese Qualität lässt sich z.B. durch den Einsatz von Applikatio-nen ermitteln, mit deren Hilfe Passwörter entschlüs-selt werden.	[in %] Anzahl Passwörter der ver-schiedenen Qualitätsstufen
Zugangskontrolle zu Netzen	Insbesondere externe Dienstleister mit der Möglichkeit, auf das Unternehmensnetzwerk zuzugreifen, sollten im Zugriff eingeschränkt sein.	[in %] Anzahl externer Dienstleis-ter, bei denen technisch sichergestellt wird, dass sie nur auf einzelne, definierte Systeme zugreifen können.

14.8 Kennzahlen im laufenden Verbesserungsprozess

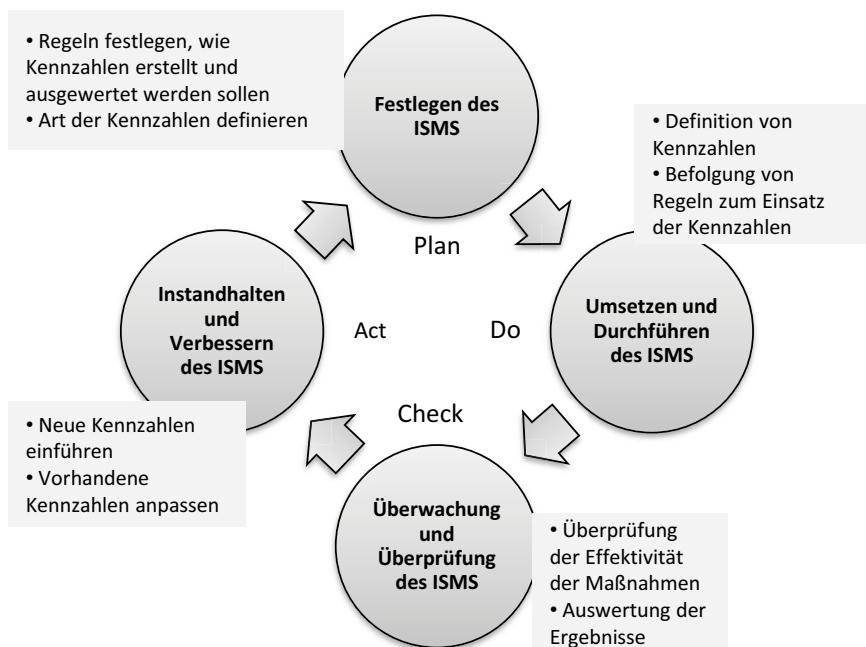
Es ist ein grundlegender Bestandteil des IT-Security-Managements, die Wirksamkeit von Maßnahmen zu messen. In der ISO 27001:2005 war noch Folgendes dazu festgehalten: »Definition eines Maßes für die Wirksamkeit der ausgewählten Maßnahmen oder Maßnahmengruppen; außerdem muss festgelegt werden, wie diese Maße benutzt werden können, um die Wirksamkeit der Maßnahmen einzuschätzen und um dabei vergleichbare und reproduzierbare Resultate zu erhalten.« In der ISO 27001:2013 ist diese Regelung in Kapitel 9 zu finden, das sich mit der allgemeinen Ermittlung der Wirksamkeit



KENNZAHLEN IM LAUFENDEN VERBESSERUNGSPROZESS

der eingesetzten Maßnahmen beschäftigt. Dort steht unter anderem, dass Maßnahmen überwacht, analysiert und ausgewertet werden müssen. Die Details werden dann in der ISO 27004 weiter ausgeführt.

Die Definition von Maßen, deren Messung, Auswertung und Darstellung ist damit ein geeignetes Mittel, um die generelle Wirksamkeit eines IT-Security-Managements und des Information-Security-Management-Systems (ISMS) zu visualisieren. Anstelle von Maßen benutzen wir im Folgenden weiterhin »Kennzahlen«.



14

Abbildung 14.3: Verwendung von Kennzahlen im PDCA-Zyklus dargestellt

In Plan-Do-Check-Act-Zyklen gedacht zieht sich die Definition der Kennzahlen durch die gesamte Do-Phase hindurch, die Messung der Wirksamkeit auf Basis der Kennzahlen ist Teil der Check-Phase.

Neue Maßnahmen, die einer Überprüfung unterzogen werden sollen, oder Veränderungen an bestehenden Messverfahren bedingen auch eine Korrektur, welche Kennzahlen eingesetzt werden und wie der Einsatz erfolgt. Aus diesem Grund sollte dieser Vorgang regelmäßig Teil des ISMS-Prozesses sein und als integraler Bestandteil gesehen werden.



14.9 Laufende Auswertung von Kennzahlen

Gute Kennzahlen sind Kennzahlen, die automatisiert erfasst und elektronisch weiterverarbeitet werden können. Dadurch wird es möglich, die betreffenden Zahlen auf Abruf oder idealerweise regelmäßig zu erheben. Standardsicherheitsprodukte wie z.B. VirensScanner, Firewalls, Netzwerkkomponenten oder Mailserver bieten dafür zentrale Datenbanken mit umfangreichen Auswertungsmöglichkeiten oder zumindest entsprechenden Protokolldateien.

Im Falle der Datenerhebung aus einer zentralen Datenbank eines Antivirussystems sind Statistiken über erkannte Viren, besonders gefährdete Unternehmensbereiche und damit eine Darstellung der allgemeinen Gefährdungslage ableitbar. Sind keine zentralen Datenbanken vorhanden und die Daten müssen aus verschiedenen Antiviren-Datenbanken zusammengebracht und logisch miteinander in Verbindung gesetzt werden, so gestaltet sich dies schon aufwendiger. Ein erster Schritt sollte also darin bestehen, alle Antiviren-Systeme und ihre Datenbanken zu identifizieren, die später ausgewertet werden sollen. Immer mit dem Blick auf die gewünschten Ergebnisse ist es dann ein weiterer Schritt, die zur Verfügung stehenden Informationen zu korrelieren und die benötigten Ergebnisse zu extrahieren. Aus den Ergebnissen wiederum lässt sich die Sicherheitslage hinsichtlich vorhandener Schadsoftware ableiten. Die Rahmenbedingungen, die eine Entscheidung hinsichtlich der Messfrequenz beeinflussen, befinden sich im Spannungsfeld von Kosten und Nutzen für die IT-Security. Dazu kommen Anforderungen an eine strategische Planung von zukünftigen Maßnahmen.

Einen weiteren Mehrwert kann man dadurch erreichen, dass man Daten unterschiedlicher Systeme miteinander in Verbindung setzt. Dem Beispiel oben folgend könnte man die Daten des Antiviren-Systems mit dem Patchmanagement koppeln. Dazu dient das SIEM, das idealerweise über eine eigene Datenbank verfügt und darüber hinaus Abfragen bereitstellt, über alle Daten hinweg Auswertungen zu erzeugen.

14.10 Annualized Loss Expectancy

Die oft genannte Kennzahl »Annualized Loss Expectancy« (ALE) bezeichnet die zu erwartenden Kosten für den Fall, dass ein Risiko tatsächlich eintritt. Der Betrachtungszeitraum umfasst ein Jahr, und Gegenstand der Betrach-



tung ist ein definierter Unternehmenswert. Mit diesem Wert sollen die negativen Effekte aller Sicherheitsvorfälle innerhalb eines Jahres bezogen auf den Unternehmenswert dargestellt werden. Wohlgemerkt: jeweils auf ein einzelnes Risiko bezogen. Beliebt ist diese Darstellung vor allem deshalb, weil sie relativ einfach zu berechnen ist und ein Gefühl von Kontrolle über die Kosten vermittelt.

Im Grunde werden zur Ermittlung der ALE die Kosten eines einzelnen Sicherheitsvorfalls (Single Loss Expectancy) mit der zu erwartenden Auftrittshäufigkeit im Zeitraum eines Jahres (Annual Rate of Occurrence) multipliziert. Die Formel stellt sich also wie folgt dar:

$$ALE = SLE * ARO$$

Der Wert *SLE* bezeichnet die Single Loss Expectancy und der Wert *ARO* stellt die Eintrittswahrscheinlichkeit pro Jahr dar.

Für die Belegung mit tatsächlichen Zahlen ist es zunächst erforderlich, den maximalen potenziellen Schaden oder Verlust zu ermitteln. Der maximale Schaden wird mit dem Ausdruck »Recovery Costs« bezeichnet. Die Recovery Costs werden z.B. im Rahmen einer Business-Impact-Analyse festgestellt. Diese Kosten beinhalten üblicherweise alle Aufwendungen, die für die vollständige Wiederherstellung aufgewendet werden müssen. Der zweite Wert beschreibt die Eintrittswahrscheinlichkeit pro Jahr. Bei der Ermittlung von Sicherheitsereignissen aufgrund von Schadsoftware ist die Ermittlung relativ einfach, da in diesem Umfeld viele Ereignisse auftreten und somit eine Einschätzung der nächsten Zukunft möglich ist. Ereignisse zu schätzen, für die keine Daten aus der Vergangenheit verfügbar sind und wo auch keine Erfahrungen vergleichbarer Unternehmen vorliegen, ist naturgemäß deutlich komplexer.

Ein weiterer Vorteil von ALE besteht darin, dass die Formel um weitere Parameter erweitert werden kann, die die Nutzungsbandbreite enorm erweitern. Eine Möglichkeit ist der Einbezug von implementierten Maßnahmen, um den positiven Effekt darzustellen. Zu diesem Zweck werden die Parameter »Wirkung von Maßnahmen« (WM) und »Kosten von Maßnahmen« (KM) eingeführt. Sowohl die Wirkung als auch die Kosten von Maßnahmen, die die Wiederherstellungskosten pro Zeiteinheit reduzieren sollen, werden auf das Jahr umgerechnet.



KAPITEL 14 – KENNZAHLEN

Die Formel wird also wie folgt erweitert:

$$ALE = (SLE - WM + KM) * ARO$$

Der Manager IT-Security kann mit dieser Formel darstellen, wie hoch die Reduzierung des ALE ausfällt, wenn eine Maßnahme implementiert wird, und diesen Wert den Kosten gegenüberstellen, die ohne diese Maßnahmen eintreten könnte. Die Herausforderung liegt nun darin, dass die Realisierung von Maßnahmen sofort budgetrelevant wird, das Eintreten eines Ereignisses aber nur mit einer gewissen Wahrscheinlichkeit in der Zukunft auftreten wird. Auch hier zeigt es sich, dass vor allem häufig auftretende Sicherheitsergebnisse in dieser Form dargestellt werden sollten.

Der Zusammenhang mit einer weiteren populären Kennzahl, des »Return on Security Investment« (ROSI) mit ALE wird deutlich, wenn man es an einem Beispiel darstellt. Auch hier macht es wieder Sinn, es an einem Beispiel aus dem Bereich Schadsoftware festzumachen. Angenommen, es entstehen Schäden von 10.000 € durch eine Attacke durch Viren. Ermittelt wurde dieser Schaden dadurch, dass der Ausfall der Produktion und damit verbundene Liefereschwierigkeiten hochgerechnet wurden. Zudem wurden Ausfälle in anderen Abteilungen mit einem im Unternehmen üblichen Stundensatz berechnet. Weiter angenommen, dieser Schaden tritt im Durchschnitt alle zwei Jahre auf, dann ergibt sich ein Verlust (Recovery Costs) von $10.000 \text{ €} / 2 = 5.000 \text{ €}$ pro Jahr. Die Installation von Virensaltern hätten die Schäden mit angenommener 95%iger Sicherheit verhindert. Daraus ergibt sich wiederum ein Einsparpotenzial (Savings) von $5.000 \text{ €} * 95 \% = 4.750 \text{ €}$. Die Installation der Antivirenssoftware inklusive Lizenzen und Wartung sowie externer Unterstützung kostet 2.000 € im Jahr.

Daraus lässt sich nun der Return on Security Investments (ROSI) errechnen:

$$ALE = Recovery Costs - Savings + Kosten der Maßnahmen$$

$$ALE = 5.000 \text{ €} - 4.750 \text{ €} + 2.000 \text{ €}$$

$$ALE = 2.250 \text{ €}$$

$$ROSI = Recovery Costs - ALE$$

$$ROSI = 5.000 \text{ €} - 2.250 \text{ €}$$

$$ROSI = 2.750 \text{ €}$$



Die Berechnung des ROSI ähnelt der üblichen Berechnung des »Return on Investment« (ROI) und ist damit eine Größe, die ein Manager IT-Security häufig überraschend gut innerhalb eines Unternehmens kommunizieren kann. Aus technischer Sicht und aus Sicht der Kennzahlen ist ALE nicht durchweg positiv zu bewerten. Betrachtet man die Kriterien für gute Kennzahlen erneut, so wird schnell ersichtlich, dass »Erwartete Kosten« und »Durchschnittliches Auftreten« nicht unbedingt verlässliches Zahlenmaterial darstellt. Kritiker drücken dies so aus: »ALE liefert präzise Ergebnisse, die auf unpräzisen Eingabedaten beruhen.« Im Endeffekt wird ALE für einige, gut bewertbare Bereiche einen guten Dienst leisten, wenn es darum geht, Ausgaben zu rechtfertigen.

Zusammengefasst lässt sich sagen, dass ALE für die Berechnung von Kosten dann sehr gut geeignet ist, sobald es sich um Sicherheitsereignisse dreht, die mit soliden Zahlen unterlegt werden können. Das ist dann der Fall, wenn eine solide Datenbasis aus den vergangenen Jahren vorliegt. In anderen Gebieten allerdings wird es der Kaffeesatzleserei Vorschub leisten und mehr Schaden in Form von Vertrauensverlust verursachen als einen positiven Effekt haben.

14

14.11 IT-Security Balanced Scorecard

Als Robert Kaplan und David Norton Anfang der 1990er Jahre die Grundlagen für die Balanced Scorecard legten, hatten sie weniger die IT-Security im Sinn. Sie wollten eine Methode entwickeln, um die Lücke zwischen der Vision eines Unternehmens und der Steuerung von strategischen Aktivitäten zu schließen. Zu den bereits seit Langem existierenden Kennzahlen aus der Finanzwelt haben sie weitere hinzugefügt. Diese weiteren Kennzahlen werden als »Perspektiven« bezeichnet, weil sie eine ausgewogenere Sicht auf die Unternehmensstrategien erlauben. Die alten wie die neu hinzugewonnenen Kennzahlen werden von einer Metaebene aus für das Unternehmen definiert, müssen aber so gestaltet sein, dass alle Ebenen von Führungskräften diese zur Entscheidungsfindung nutzen können.

Die Erkenntnis, dass es wichtig ist, Aktivitäten aller Art in der IT-Security zu messen und zu steuern, hat sich erst einige Jahre später auf breiter Basis durchgesetzt. Dennoch stellt die Balanced Scorecard eine Methodik zur Verfügung, die es dem Manager IT-Security erlaubt, mithilfe von Kennzahlen den Fortschritt von Prozessen hin zur Erreichung definierter Ziele darzustellen.



Da sich die Balanced Scorecard im betriebswirtschaftlichen Umfeld weitgehend durchgesetzt hat, stellt sie auch im Umfeld der IT-Security einen Weg dar, der häufig schnelle Anerkennung und Wiedererkennbarkeit garantiert. Letztendlich ist das Ziel, die Kontrolle über alle Aktivitäten im IT-Security-Umfeld zu erlangen und im Hinblick auf übergeordnete Security-Strategien und Ziele zu steuern. Damit stellt sie ein Führungsinstrument dar und wird zum Bereich der IT-Governance gezählt.

Die klassische, betriebswirtschaftlich geprägte Business Scorecard wird aus vier Perspektiven betrachtet, deren Ausgewogenheit auf ständiger Kontrolle und Anpassung basiert. Die vier Perspektiven sind die Finanzperspektive, die Kunden- und Lieferantenperspektive, die interne oder Prozessperspektive sowie die Wachstumsperspektive, auch als Potenzialperspektive bezeichnet. Eine IT-Security Balanced Scorecard wird sinnvollerweise dieselben Perspektiven nutzen wie die klassische Balanced Scorecard. Das oberste Ziel im IT-Security-Umfeld wird die Sicherstellung von Vertraulichkeit, Verfügbarkeit und Integrität aller Werte sein.

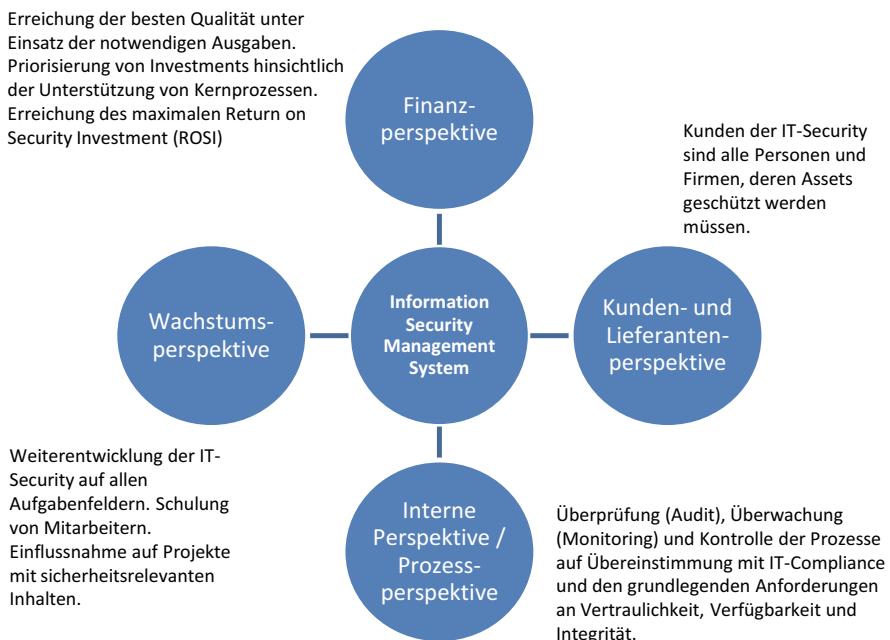


Abbildung 14.4: Perspektiven der Balanced Scorecard



Nun stellt sich automatisch die Frage, ob es nicht sinnvoll wäre, diese sehr IT-Security-fernen Perspektiven durch mehr technisch geprägte zu ersetzen. Man könnte sich durchaus auch Perspektiven vorstellen wie

- Bedrohungsmanagement
- Verwundbarkeitsmanagement
- Zugriffsmanagement
- IT-Risikomanagement
- IT-Compliance-Management usw.

Der Nachteil einer solchen Herangehensweise wäre zum einen der rein technische Blick, den man wiederum durch weitere Perspektiven abmildern könnte, und zum anderen der, dass man sich damit von der klassischen Balanced Scorecard entfernen würde. Damit würden sich auch die Vorteile wieder relativieren, die sich aus einer gemeinsamen Sprache mit den Betriebswirten ergeben.

14

14.11.1 Einführung der IT-Security Balanced Scorecard

Bei der Erstellung und dem Einsatz einer IT-Security Balanced Scorecard wird eine Vorgehensweise gewählt, die es erlaubt, jeden Schritt nachvollziehbar zu gestalten. Exemplarisch wird anhand des »Nine-Steps-Models« des Balanced Scorecard Institutes aufgezeigt, wie die verschiedenen Schritte ineinander übergehen.

Die Balanced Scorecard, in unserem Fall als Unterart die IT-Security Balanced Scorecard, ist mehr als nur ein Verwaltungswerkzeug für Maßnahmen. Als solches würde es auch am Widerstand der verschiedenen Interessenslagen im Unternehmen scheitern. Die IT-Security Balanced Scorecard ist vielmehr ein Managementinstrument. Es ist erforderlich, dass ein Top-down-Verständnis vorhanden ist, dass die Ziele der IT-Security und die zu erarbeitenden Soll-Ergebnisse für das Unternehmen von Wert sind und dass dafür die damit verbundenen Aufwände aufgebracht werden müssen. Auf einer darunter liegenden Ebene müssen die Führungsebenen die IT-Security Balanced Scorecard leben und in ihre tägliche Führungsarbeit mit aufnehmen. Schlussendlich muss auch der durchführende Mitarbeiter seine Arbeit entsprechend den Zielen der Scorecard priorisieren, abarbeiten und den Regeln entsprechend rückmelden.



Vorarbeiten

Schritt 1: Ist-Aufnahme

Zu Beginn steht die Bestandsaufnahme. Wo will das Unternehmen hin und welche Visionen und Strategien sollen verfolgt werden? Dazu gehört auch die Identifikation der grundlegenden Ziele der Unternehmensführung hinsichtlich der IT-Security. Grundsätzlich fließen in diesen Schritt auch bereits Vorgaben ein, die im Zuge der IT-Compliance als strategisch wichtig erachtet werden. Folgende Punkte werden in diesem Zusammenhang aufgeführt:

- **Mission (mission):** Warum ein Unternehmen am Markt ist und welchen Mehrwert es für die Allgemeinheit bringt
- **Werte (values):** Die Werte, an die sich ein Unternehmen hält, wenn es agiert
- **Vision (vision):** Eine Vorstellung davon, wohin es gehen soll unter Fortführung der Mission
- **Strategie (strategy):** Die Aktivitäten, die dem Unternehmen helfen sollen, Visionen umzusetzen

14

Ein weiterer Faktor, der in die Überlegungen als Input mit eingebracht werden kann, ist das Ergebnis der Business-Impact-Analyse: die Definition und Priorisierung der wichtigsten Geschäftsprozesse.

Grundsätzliche Überlegungen und daraus resultierende Entscheidungen, wie die IT-Security Business Scorecard final gestaltet und im Unternehmen angepasst werden soll, müssen zu Beginn der Umsetzung getroffen werden. In großen Unternehmen sind zudem häufig kulturelle und organisatorische Unterschiede zu beachten.

Ein weiterer Punkt wird häufig unterschätzt. Bevor eine IT-Security Balanced Scorecard wirkungsvoll eingebunden werden kann, muss ein Change-Management existieren, auf das aufgebaut werden kann. Dazu gehört eine Vorgehensweise zur Kommunikation, zum Informationsaustausch und darauf aufbauend die geeigneten Workflows. Das Change-Management sorgt für kontrollierte und effiziente Änderungen an IT-Prozessen oder der IT-Infrastruktur und ist damit das Vehikel, das zur Umsetzung von Anforderungen benötigt wird.



Schritt 2: Strategie

Abgeleitet von der Ist-Aufnahme werden im zweiten Schritt die strategischen Ziele in Form von Workshops erarbeitet. Im Fokus stehen dabei die grundlegenden Anforderungen, die sich aus den wichtigsten Unternehmenszielen ableiten lassen. In diesem Schritt wird ein »übergeordnetes Bild« (*bigger picture*) erarbeitet.

Schritt 3: Maßnahmenziele erarbeiten

Die in den ersten beiden Schritten definierten Visionen werden in Schritt drei für alle Perspektiven in qualitative Ziele umgesetzt. Dafür werden die Maßnahmenziele zunächst einer der zuvor ermittelten, übergeordneten Strategie zugeordnet und dann nach Perspektive kategorisiert. Eine einfache Ursache-Wirkung-Untersuchung stellt zudem die Abhängigkeit von anderen Maßnahmenzielen dar. Die Maßnahmenziele müssen dabei laufend an sich ändernde Unternehmensziele angepasst werden.

14

Schritt 4: Strategieübersicht

Der vierte Schritt steht im Zeichen der Aufstellung einer kompletten Strategieübersicht. Auf ihr finden sich alle Unternehmensziele, die daraus abgeleiteten Maßnahmenziele und ihre Beziehungen zueinander, wiederum kategorisiert nach den Perspektiven. Die jetzt generierte Übersicht spiegelt den Bottom-up-Ansatz wider, wie durch Umsetzung geeigneter Maßnahmen die Ziele der IT-Security erreicht werden sollen und wie diese wiederum im Gesamtkontext der Unternehmensziele stehen.

Schritt 5: Kennzahlen festlegen

Bislang wurden Ziele definiert und mit Maßnahmen unterfüttert. Um den Erfolg messen zu können, führt Schritt fünf die dafür erforderlichen Kennzahlen ein. Für jedes strategische Maßnahmenziel muss mindestens eine definiert werden. Zusätzlich zur reinen Kennzahl wird der Ausgangswert (*baseline*) ermittelt und Vergleichszahlen (*benchmark*) festgelegt, anhand deren eine Überprüfung stattfinden kann.

Schritt 6: Verantwortlichkeiten festlegen

Für jedes Maßnahmenziel, jede Maßnahme und jede Kennzahl muss es eine verantwortliche Stelle geben, die in einer Übersicht festgehalten wird. Das



Gleiche gilt für die laufende Überarbeitung der Maßnahmenziele, die sich von sich ändernden Unternehmensstrategien ableiten und damit einem Änderungsprozess unterworfen sind.

Schritt 7: Softwaregestützte Einführung der IT-Security Balanced Scorecard

Durch entsprechende Software wird sichergestellt, dass alle Informationen zur richtigen Zeit zu den richtigen Personen gelangen. Software definiert den Rahmen und die zu erfassenden Werte. Die Auswahl des richtigen Softwareprodukts ist für den Erfolg essenziell. Aus diesem Grund findet üblicherweise erst in dieser Stufe eine Evaluierung von verschiedenen Produkten statt. Die Software muss vorrangig die zusammengetragenen Visionen, Maßnahmenzielen und Kennzahlen verarbeiten und in geeigneter Weise darstellen können. Des Weiteren muss sie unternehmensweit einsetzbar sein.

14

Einführung

Schritt 8: Kaskadierung

Bislang wurden alle aufgestellten Pläne Top-down, also aus Sicht des Unternehmens betrachtet. In Schritt acht findet nun der Prozess statt, die Scorecards bis auf Abteilungsebene und am Schluss bis auf Team- und Mitarbeiterebene herunterzubrechen. Das Ziel muss sein, dass jeder beteiligte Mitarbeiter seine tägliche Arbeit mit einer Scorecard verbinden kann. Dazu ist es erforderlich, dass sich Unternehmensvisionen zu Maßnahmenzielen entwickeln, die wiederum in ganz konkreten Maßnahmen und Arbeitsabläufen münden. Neben diesen werden auch die entwickelten Kennzahlen den Arbeitsabläufen zugeordnet. Nur wenn dieser Umbruch funktioniert, kann die IT-Security Balanced Scorecard im Unternehmen bestehen.

Schritt 9: Überprüfung

Durch Hinterfragen der zugrunde liegenden Festlegungen werden die Scorecards überprüft. Die Überprüfung beginnt ganz oben bei der Abfrage der Unternehmensstrategie. Fragestellungen wie »Funktioniert die Unternehmensstrategie?« oder »Investieren wir das IT-Security-Budget so, dass es die strategischen IT-Security-Ziele unterstützt?« müssen beantwortet werden.



14.11.2 Maßnahmenziele für den Bereich IT-Security

Für alle Aufgabenfelder der IT-Security können Maßnahmenziele für alle in der Praxis üblichen Perspektiven entwickelt werden. Das zeigt, dass es nicht zwingend erforderlich ist, die üblichen, betriebswirtschaftlich geprägten Perspektiven durch mehr technisch orientierte zu ersetzen.

Aufgabenfeld der IT-Security	Perspektive	Beschreibung
Awareness und Schulung	Finanzperspektive	Weniger Sicherheitsvorfälle aufgrund von besserer Schulung der Mitarbeiter. Vermeidung von Fehlern aufgrund von Nichtwissen.
	Kunden- und Lieferantenperspektive	Mitarbeiter wissen um die Sicherheitsbelange der Kunden und Lieferanten und erzeugen dadurch Vertrauen und vermitteln Kompetenz. Mitarbeiter wissen, welche technischen Tools und Verfahren im Umgang mit Informationen des Kunden und Lieferanten genutzt werden müssen.
	Interne Perspektive/Prozessperspektive	In Projekten werden die Vorgaben aus der IT-Security mit eingebunden.
	Wachstumsperspektive	Die Awareness bei den Mitarbeitern, aber auch Lieferanten wird gesteigert.
IT-Risikomanagement	Finanzperspektive	Finanzielle Verluste aufgrund von Sicherheitsvorfällen werden verringert.
	Kunden- und Lieferantenperspektive	Das IT-Risikomanagement adressiert Kunden- und Lieferantendaten und vermeidet dadurch, dass interne Schwachstellen zu Sicherheitsvorfällen bei Kunden oder Lieferanten führen.
	Interne Perspektive/Prozessperspektive	Das IT-Risikomanagement trägt Sorge, dass die internen Prozesse und die darunterliegenden IT-Systeme störungsfrei funktionieren.



KAPITEL 14 – KENNZAHLEN

14

Aufgabenfeld der IT-Security	Perspektive	Beschreibung
	Wachstumsperspektive	Das IT-Security-Management unterstützt den Lernprozess, indem Sicherheitsvorfälle dokumentiert und die Sicherheitsprozesse dementsprechend angepasst werden.
Zugriffs-kontrolle	Finanzperspektive	Der Zugriff auf Systeme, deren Missbrauch zu finanziellem Schaden führen könnte, wird eingeschränkt.
	Kunden- und Lieferan-tenperspektive	Der Zugriff auf Kunden- und Lieferanten-systeme wird auf den Personenkreis beschränkt, der diesen Zugriff benötigt.
	Interne Perspektive/ Prozessperspektive	Der Zugang zu IT-Systemen und Werten wird in der Form geregelt, dass jeder Zugang nur dann eingerichtet wird, wenn er zur Erfüllung der Aufgabe erforderlich ist.
	Wachstumsperspektive	Benutzer erhalten den Zugang, den sie benötigen, um im Sinne des Geschäftszwecks tätig zu werden.
Business Continuity Management	Finanzperspektive	Im Falle von Notfällen greifen Notfallprozeduren, die den Geschäftsablauf gemäß der Service Level Agreements gewährleisten.
	Kunden- und Lieferan-tenperspektive	Im Notfall wird die Abarbeitung von Dienstleistungen für den Kunden gewährleistet. Der Zugang zu Dienstleistungen der Lieferanten bleibt erhalten.
	Interne Perspektive/ Prozessperspektive	Das Business Continuity Management wird weiterentwickelt und getestet.
	Wachstumsperspektive	Alle beteiligten Mitarbeiter wissen um ihre Aufgaben und Rollen im Rahmen des Business Continuity Managements.



IT-SECURITY BALANCED SCORECARD

Aufgabenfeld der IT-Security	Perspektive	Beschreibung
IT-Compliance	Finanzperspektive	Das Unternehmen arbeitet gemäß den IT-Compliance-Vorgaben.
	Kunden- und Lieferantenperspektive	Vereinbarungen mit Kunden und Lieferanten werden eingehalten. Dazu gehören alle vertraglichen wie gesetzlichen Regelungen. Insbesondere Liefertreue und Qualität sind in diesem Umfeld zu untersuchen.
	Interne Perspektive/Prozessperspektive	Betroffene Mitarbeiter kennen die für sie und ihre Arbeit geltenden Bestimmungen.
	Wachstumsperspektive	IT-Compliance-Maßnahmen werden laufend überprüft und angepasst.





15 Praxis: Aufbau eines ISMS

15.1 Kapitelzusammenfassung

Erläutern die bisherigen Kapitel die verschiedenen Aufgabenbereiche des Managers IT-Security, so folgt nun die praxisnahe Beschreibung des Aufbaus oder der Weiterentwicklung eines bestehenden ISMS.

Wichtig

Alle Tätigkeiten, die dem IT-Security-Management zugeordnet werden können, sind Tätigkeiten, die im Rahmen des Information-Security-Management-Systems (ISMS) stattfinden. Das ISMS bietet demnach den Rahmen, die Vorgehensmodelle und das normierte Fundament für das IT-Security-Management. Damit stellen alle Themen, die in den verschiedenen Kapiteln des vorliegenden Buches behandelt werden, Puzzleteile sowohl des IT-Security-Managements als auch des ISMS dar.

Im Gegensatz zu den Teilbereichen der IT-Security, die durchaus einzeln angegangen werden können, ist für den Aufbau und Betrieb eines ISMS eine geordnete Vorgehensweise zu empfehlen. Eine mögliche Vorgehensweise wird im aktuellen Kapitel beschrieben.

Die Top-6-Fragen zum aktuellen Kapitel

- Stehen die Risiken, die die Vertraulichkeit, Verfügbarkeit und die Integrität der Unternehmenswerte gefährden, im Vordergrund und werden diese dokumentiert?
- Sind die einzelnen Unternehmenswerte bekannt, die durch die IT-Security-Organisation geschützt werden sollen? Existieren entsprechende Dokumentationen, auf die sich der Manager IT-Security beim Aufbau eines ISMS stützen kann?
- Ist das IT-Security-Management in ein existierendes ISMS eingebettet?



KAPITEL 15 – PRAXIS: AUFBAU EINES ISMS

- Wird für den Betrieb des ISMS ein Tool eingesetzt?
- Werden die Entscheidungen, Maßnahmen, Risiken und alle weiteren Ergebnisse aus dem IT-Security-Management dokumentiert?
- Ist ein kontinuierlicher Verbesserungsprozess nach dem PDCA-Modell implementiert und hilft er dabei, das Sicherheitsniveau nachdrücklich und nachweislich laufend zu erhöhen?

15.2 Einführung

Gleichgültig, welchen Unternehmenszweck ein Unternehmen verfolgt, und auch weitgehend unabhängig davon, wie groß ein Unternehmen ist, ist es stets sinnvoll, den Bereich IT-Security nach anerkannten Standards auszurichten. Wie des Öfteren in diesem Buch erwähnt, sind es vor allem zwei Normen, die hinsichtlich des Betriebs eines Information-Security-Management-Systems (ISMS) maßgeblich von Bedeutung sind: Die ISO-2700x-Normen und die Standards, die vom Bundesamt für Sicherheit in der Informations-technik (BSI) herausgegeben werden. Nicht sehr überraschend ist, dass sich diese beiden Vorgehensmodelle – zumindest, was die Ausgestaltung auf Pro-zessebene und den Umgang mit Maßnahmen betrifft – weitgehend einander angenähert haben.

Ein weiteres Ziel, das zunehmend immer mehr Unternehmen beschäftigt, ist die Frage des Nachweises, dass sie IT-Security nicht nur auf der Agenda haben, sondern dass diese auch solide gelebt wird und dies auch anhand einer Zertifizierung durch eine anerkannte Stelle nachgewiesen werden kann. Diesen Nachweis kann wiederum sowohl eine Organisation bieten, die nach ISO 27001 zertifiziert, als auch das BSI, das die Zertifizierung »ISO 27001 auf der Basis von IT-Grundschutz« anbietet. Als Grundlage für die Abnahme des IT-Security-Managements dient in beiden Fällen ein funktionierendes ISMS.

15.3 ISMS in Kürze

Als Erstes muss ein Satz wiederholt werden, der, auch wenn er langsam abgedroschen klingt, die Kernaussage der IT-Security auf den Punkt bringt: »IT-Security ist keine Software, kein Werkzeug und auch kein Zustand. IT-Security ist ein Prozess!« Diese Feststellung ist nicht neu und eigentlich auch durch jeden mit der Thematik Befassten leicht einsehbar. Dennoch wird



immer wieder gefragt, wo man denn ein ISMS erwerben kann. Die Antwort darauf lautet: Das ISMS ist die Umsetzung von IT-Security in einem Unternehmen, und damit ist es auch kein Produkt, sondern ein stetiger Prozess.

Natürlich gibt es Software, die den Betrieb eines ISMS unterstützt. Das tut sie aber auch nur dann, wenn sie zuvor mit Daten wie den eigenen (Unternehmens-)Werten, Risikobetrachtungen, Maßnahmen und Richtlinien gefüllt wurde. Der Weg zu einem gefüllten und betriebsbereiten ISMS-Softwaresystem kann ebenfalls durch Wizards, Formulare oder bereits fertige Workflows vonseiten des Herstellers unterstützt werden. Ohne Fachwissen, eine genaue Zielsetzung und erheblichen Aufwand wird man dennoch nicht auskommen.

Die Aufgabe eines Managers IT-Security ist der Betrieb des IT-Security-Managements. Das Vorgehensmodell, also die Methodik und die Definition der Prozesse, werden mithilfe des ISMS definiert und gelebt. Daneben dient es als Datenbank für alle Arten von Informationen aus der IT-Security und stellt damit den Dreh- und Angelpunkt dar.

Wichtig

Ein ISMS ist nach Definition durch die ISO 27001 »der Teil des gesamten Managementsystems, der auf der Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überprüfung, Instandhaltung und Verbesserung der Informationssicherheit abdeckt«. Ergänzt wird diese Beschreibung durch folgende Anmerkung: »Das Management- system enthält die Struktur, Grundsätze, Planungsaktivitäten, Verantwortung, Praktiken, Verfahren, Prozesse und Ressourcen der Organisation.«

Grundsätzlich hat das ISMS zum Ziel, ein angemessenes und von der Unternehmensleitung gefordertes Niveau an Sicherheit für die schützenswerten Werte des Unternehmens zu erreichen.

Die Definition eines ISMS nach ISO 27001 zeigt auf, welche Aufgabenbereiche in dessen Rahmen gesehen werden:

- Das IT-Risikomanagement ist die zentrale Methodik zur Ermittlung, Bewertung und Abwehr von Risiken.
- Aufbau und Entwicklung eines IT-Security-Managementsystems mit den Komponenten:



KAPITEL 15 – PRAXIS: AUFBAU EINES ISMS

- 15
- Organisationsstruktur (»Verantwortung«),
 - Richtlinienstruktur (»Verfahren«),
 - den Prozessen aus der technischen IT-Security und dem allgemeinen Betrieb (»Prozesse«),
 - die Überwachung mithilfe von Audits, Kennzahlen und dem Monitoring (»Überprüfung« und »Überwachung«),
 - die Dokumentation,
 - die kontinuierliche Verbesserung im Allgemeinen und die Aufrechterhaltung des Betriebs im Rahmen der Aktivitäten zum IT Business Continuity Management (»Instandhaltung und Verbesserung«),
 - Verbesserung von Awareness und Durchführung von Schulungen im Rahmen der Verbesserung und
 - ergänzt durch die Anmerkung, dass selbst der Betrieb eines ISMS nach ISO 27001 es nötig macht, jede Handlung nach Übereinstimmung mit geltenden Vorgaben wie Gesetzen zu überprüfen, was wiederum die Thematik IT-Compliance anspricht.

Wie aus der Definition bereits herauszulesen ist, handelt es sich bei einem ISMS um eines von möglicherweise mehreren Managementsystemen innerhalb eines Unternehmens. So ist die Integration mit bestehenden Managementsystemen wie einem Qualitätsmanagementsystem oder einem Datenschutz-Managementsystem von vornherein angedacht, und dies dürfte auch ein Grund dafür sein, warum wesentliche Mechanismen der ISO 27001 wie der Plan-Do-Check-Act-Zyklus analog zur ISO 9001 aufgebaut sind. Synergieeffekte, die aus bereits bestehenden Methoden abgeleitet werden können, sollten in jedem Fall genutzt werden.

Wichtig

Der Aufbau eines ISMS, der in allen Facetten auch den Vorgaben von Normen entspricht, ist immer aufwendig und damit auch kostenintensiv. Je näher man an den zertifizierbaren Standard ISO 27001 heranrückt, desto lückenloser muss die Umsetzung sein und desto mehr steigt der Aufwand. Eine ganze Reihe interner Organisationseinheiten werden sich intensiv mit der Thematik beschäftigen und ihre Arbeitskraft einbringen müssen. Das gilt sowohl für die Planung und den Aufbau als auch den



Betrieb des ISMS. Den Auftrag zu einer solchen Vorgehensweise zu erteilen und auch die erforderlichen Ressourcen zur Verfügung zu stellen, ist Aufgabe der Unternehmensleitung.

Die Grundlage für Aktivitäten, die im Rahmen eines ISMS angestoßen werden, ist die Analyse und Bewertung durch die Methoden des Risikomanagements. Das Risikomanagement wird als das Werkzeug beschrieben, das festlegt, welche Maßnahme in welchem Umfang implementiert wird. Alle nachfolgend genannten Teilbereiche eines ISMS basieren damit auf der Risikoanalyse und der Risikobewertung. Diese Feststellung charakterisiert das ISMS nach ISO 2700x wie keine andere.

15

15.4 Herangehensweise

Die verschiedenen Kapitel des vorliegenden Buches bieten jeweils den Einblick in einen Teil des Gesamtkomplexes IT-Security-Management und die Aufgaben des Managers IT-Security. Zusammengehalten werden diese einzelnen Themenfelder durch die Klammer ISMS. Das Zusammenfügen zu einem Ganzen folgt einer eigenen Systematik, die letztendlich nicht nur den reinen Aufbau gewährleisten soll, sondern auch den darauf folgenden Betrieb unterstützen muss. Das Vorgehensmodell nennt sich Plan-Do-Check-Act-Zyklus und hilft dabei, zum richtigen Zeitpunkt den richtigen Schritt zu vollziehen.

Während der Aufbauphase eines neuen ISMS stellt sich immer die Frage, was schon alles an verwertbaren Informationen und Strukturen im Unternehmen existiert. Erst wenn diese Frage geklärt ist, können die Aufwände für alle weiteren Schritte geklärt werden. Ist bereits eine IT-Security-Organisation etabliert und arbeitet weitgehend optimal, so ist nur noch zu überlegen, ob die übergeordnete Zielsetzung ausreichend formuliert wurde und ob im Rahmen dieser Zielsetzung bereits alle davon abzuleitenden Aufgaben für das IT-Security-Management in den Betrieb übergegangen sind.

Der Aufbau eines neuen ISMS und die Verbesserung eines bestehenden ISMS unterscheiden sich hinsichtlich der Vorgehensweise kaum. Immer geht es ursächlich darum, die Ist-Situation zu erfassen, zu bewerten, das Delta zwischen Soll und Ist zu ermitteln und daraus wiederum weitere Schritte abzulei-



ten. Dieser universelle Ansatz macht die Vorgehensweise im Kontext des Plan-Do-Check-Act-Zyklus so beliebt.

Tipp

Der Blick durch die Brille eines unabhängigen Dritten kann in jedem Fall helfen, eine neue Sicht auf die Belange und die davon abgeleiteten Maßnahmen zu gewinnen. Diese Option sollte vor allem deshalb auch angedacht werden, weil der Aufwand eines solchen Projekts immens sein kann und somit kaum Raum für Fehlentscheidungen vorhanden ist.

15

Eine Herangehensweise mit Checkliste, die darauf ausgelegt ist, ein einmalig überprüfbares Ergebnis herbeizuführen, wird auch nur zum Stichtag ein akzeptables Sicherheitsniveau garantieren können. Der technische Fortschritt und die vielen kleinen und großen Änderungen an IT-Prozessen und IT-Systemen erfordern ein konsequentes Nachhalten, Nachprüfen und Nacharbeiten – drei Stichworte, die gut als die drei wesentlichen Merkmale eines ISMS herhalten können. Daraus kann auch der personelle Aufwand abgeleitet werden, den der Betrieb eines ISMS mit sich bringt. Einsparungen an dieser Stelle werden in den meisten Fällen direkt zu eingeschränkter Leistungsfähigkeit und damit einem niedrigeren Sicherheitsniveau führen. Auf der anderen Seite wird dadurch auch deutlich, welch hoher Stellenwert die professionelle Implementierung und die Schaffung der Basis für den Betrieb hat. Nicht zielgerichtete und ineffiziente ISMS-Prozesse führen fast unweigerlich zu unnötig hohen Aufwänden – Ressourcen, die dann an anderer Stelle fehlen.

Jede Vorgehensweise muss an die Rahmenbedingungen angepasst werden, die in einem Unternehmen vorherrschen. Jedes Unternehmen tickt anders, und so wird auch das Projekt zur Einführung oder Verbesserung des ISMS jeweils anders gestaltet werden.

15.5 Schritt für Schritt zum ISMS

Bislang wurde viel von der IT-Security-Organisation und den Aufgaben geschrieben, um die sie sich kümmern sollte. Aufgabenstellungen wie das IT-Risikomanagement oder auch technische Aspekte wurden erklärt. Nun



SCHRITT FÜR SCHRITT ZUM ISMS

ist es an der Zeit, diese Einzeldisziplinen in einen Gesamtzusammenhang zu bringen.

Den Rahmen für diesen Zusammenhang bildet die Aufgabenstellung, in einem Unternehmen ein ISMS einzuführen und zu betreiben. Grundsätzlich folgen die einzelnen Schritte auf dem Weg dorthin einer gewissen Logik, da sie insofern voneinander abhängig sind, als dass der Output des einen Schritts als Input des nächsten genutzt werden kann. In Abbildung 15.1 werden die einzelnen Schritte auf der linken Seite des Schaubildes gezeigt, während eine Zuweisung zu den verschiedenen Aufgaben der IT-Security-Organisation auf der rechten Seite stattfindet. Um den Querverweis auf die jeweiligen Stellen im Buch zu erleichtern, wurden zusätzlich Angaben über das jeweilige Kapitel mit eingefügt.

15

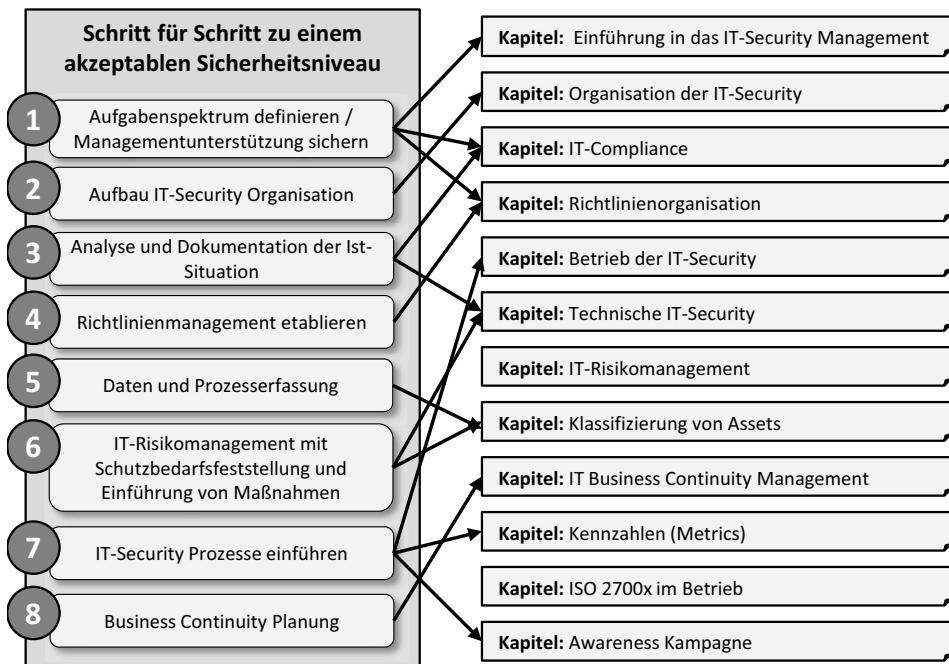


Abbildung 15.1: Aufbau ISMS und die Aufgabenfelder der IT-Security

Da jedes Unternehmen eine andere Zielsetzung verfolgt und schon von der Struktur und Aufbauorganisation her nicht miteinander vergleichbar ist, wird



KAPITEL 15 – PRAXIS: AUFBAU EINES ISMS

die Darstellung so weit abstrahiert, dass sie sowohl auf kleinere Unternehmen als auch auf größere Unternehmen anwendbar ist.

Wichtig

Den Unterschied zwischen der einmaligen Abarbeitung der einzelnen Schritte und einem gelebten ISMS macht die stetige Überprüfung aller Teilbereiche der IT-Security. So beinhaltet ein Audit, das Monitoring, das IT-Risikomanagement und alle weiteren Themen jeweils die Frage, ob denn etwas an den bestehenden Prozessen oder Bewertungen angepasst werden sollte. Diese Nabelschau führt dann wiederum zu Maßnahmen, die eine erneute Abarbeitung ausgewählter Schritte erforderlich machen können.

15

Wie in der Einführung zu diesem Kapitel erwähnt, werden die Normen ISO 2700x und die Standards des BSI für den Aufbau Pate stehen. Da auch diese beiden Normen ihre Ecken und Kanten haben, werden zusätzlich Erfahrungen aus eigenen Projekten einfließen, um diese Ecken und Kanten abzumildern und an die gelebte Unternehmenswirklichkeit anzunähern.

In Abbildung 15.2 wird ein Zusammenhang zwischen dem Aufbau eines ISMS und den damit befassten Normen hergestellt. So werden neben der allgegenwärtigen ISO 27001 auch die anderen Normen der ISO-2700x-Reihe in einen Kontext gebracht. Ein wichtiges Symbol ist der unten links abgebildete Regelkreis. Dieses unscheinbare Konstrukt deutet eine entscheidende Dimension des ISMS an: den kontinuierlichen Verbesserungsprozess, innerhalb dessen sich der Betrieb des ISMS laufend bewegen wird. Diesen Verbesserungsprozess nennt man in der Normensprache »Plan-Do-Check-Act-Zyklus« oder auch abgekürzt »PDCA-Regelkreis«. Er wird in Folge noch häufiger erwähnt.

Jedes Projekt wie auch die Einführung eines ISMS wird in irgendeiner Form einem Projektplan mit vielen aufeinanderfolgenden Einzelschritten folgen. Die einzelnen Schritte werden dabei immer wieder von vorausgehenden abgeschlossenen Aufgaben abhängig sein und die Basis für die nächsten Herausforderungen bilden. Erst werden die Grundlagen geschaffen, um dann die einzelnen Bereiche aufzubauen. So wird z.B. erst eine generelle Zielsetzung festgeschrieben werden müssen, bevor ein Richtlinienmanagement aufgebaut werden kann, von dem wiederum die Durchführungsmethodik von



SCHRITT FÜR SCHRITT ZUM ISMS

Audits abhängt. Die seriellen und voneinander abhängigen Schrittfolgen wiederum werden zum Teil parallelisiert, wie es in jedem größeren Projekt der Fall ist. Dies ist schon deshalb erforderlich, um die für das Projekt zur Verfügung gestellten Ressourcen effektiv zu nutzen.

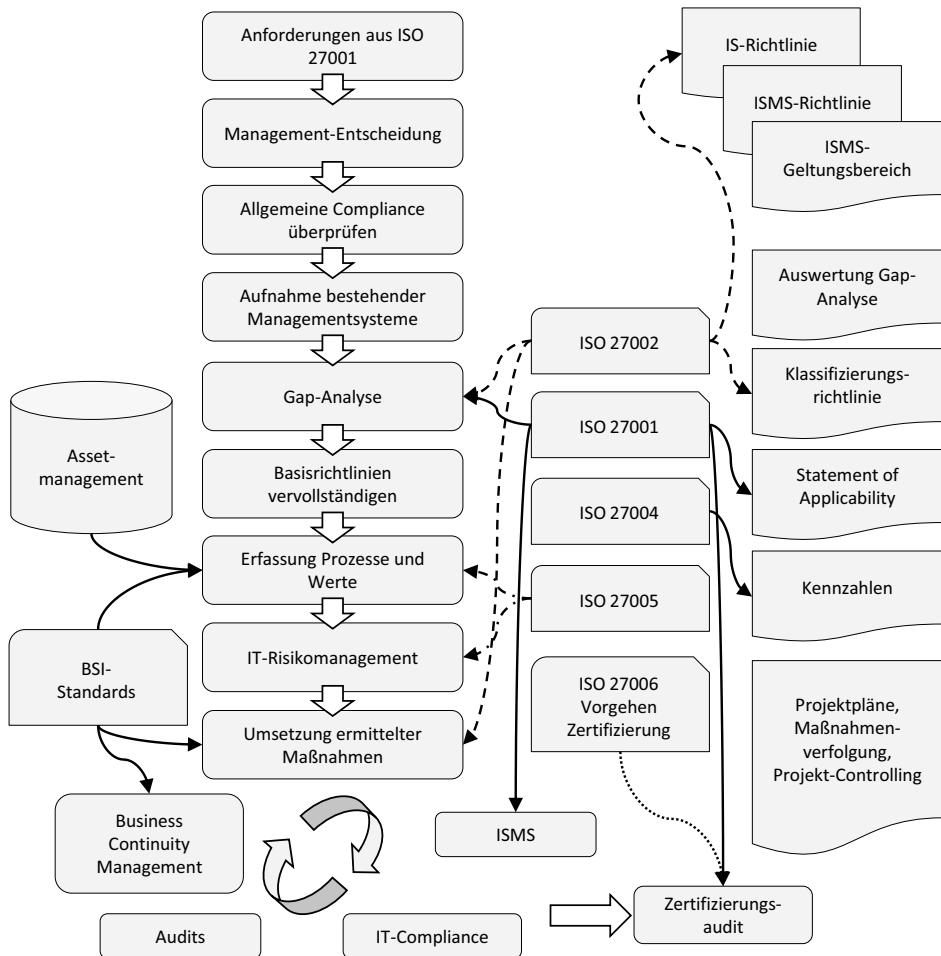


Abbildung 15.2: Zusammenhang Einführung ISMS und verschiedene Standards

Übergeordnet über die verschiedenen Teilprojekte und Arbeitsschritte ist die generelle Vorgehensweise anhand des PDCA-Zyklus zu sehen. Aus diesem Grund wird in den entsprechenden Abschnitten das Vorgehen anhand dieses Regelkreises beschrieben. Die beiden Sichtweisen, also Vorgehensweise nach



KAPITEL 15 – PRAXIS: AUFBAU EINES ISMS

Projektplan und Durchführung auf Basis eines Regelkreises, widersprechen sich nicht, und die klassische Form der Projektvorgehensweise wird dadurch nicht abgelöst. Es ist aber von vornherein wichtig, also schon in der Projektphase, die Einzelstationen des PDCA-Zyklus zu verinnerlichen. Aus diesem Grund wird auch in der ISO 27001 der Aufbau eines ISMS in dieser Form beschrieben. In der Praxis hat es sich zudem bewährt, die Denkweise und Nomenklatur der entsprechenden Standards frühzeitig in das Projekt zu übernehmen. Auf diese Weise sind Denkfehler oder schlicht Versäumnisse in Projekten schon häufig im Rahmen einer Überprüfungsphase aufgefallen, die ansonsten erst zu Beginn des Betriebs sichtbar geworden wären.

15.5.1 Plan-Do-Check-Act

15

Auch wenn den Projektmitgliedern und den Auftraggebern des Projekts bereits bewusst ist, welche Bestandteile eines IT-Security-Managements innerhalb des Projekts aufgesetzt und später in den Betrieb übernommen werden sollen, so ist zunächst die Frage zu klären, wie dies vonstatten gehen soll. Die Frage nach dem »Wie« beantwortet die Vorgehensweise nach Plan-Do-Check-Act (PDCA). Der Projektablauf nach PDCA folgt einem Prozess, in dem Einzelschritte jeweils den Output des vorangegangenen Schritts aufnehmen und den Input für den nächsten Schritt vorbereiten.

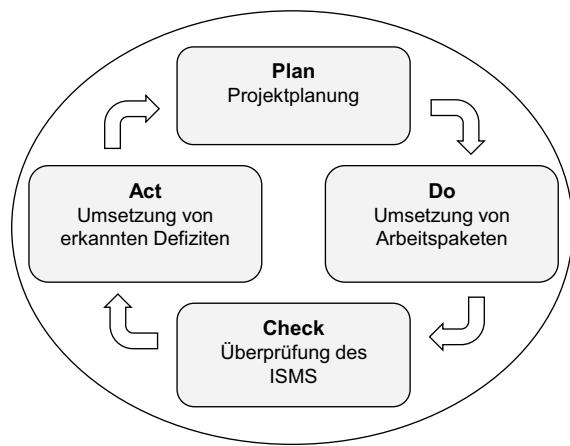


Abbildung 15.3: PDCA auf oberster Ebene

Der PDCA-Kreislauf ist bereits aus anderen Normen bekannt, unter anderen der ISO 9001. Dies hat den Vorteil, dass es mit hoher Wahrscheinlichkeit



bereits eine Organisationseinheit im Unternehmen gibt, die sich damit detailliert beschäftigt hat. Auch auf Ebene der Unternehmensleitung wird die Vorgehensweise damit leichter zu verargumentieren sein.

In Abbildung 15.3 ist ein PDCA-Kreislauf abgebildet, der die generelle Vorgehensweise von einer Metaebene aus gesehen beschreibt. Die kontinuierliche Verbesserung des IT-Security-Managements ist dadurch gekennzeichnet, dass jeder Implementierung, in diesem Fall der Installation eines ISMS, immer eine Phase der Überprüfung und anschließend der Verbesserung folgt.

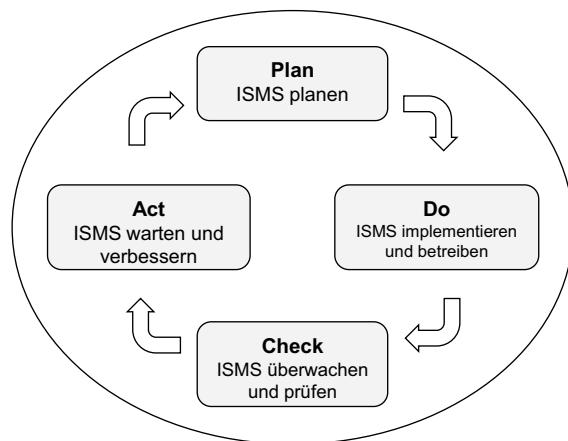


Abbildung 15.4: PDCA bei der Einführung oder Erweiterung eines ISMS

In Abbildung 15.4 ist der PDCA-Kreislauf zu sehen, wie er bei Einführung oder aber Erweiterung eines bestehenden ISMS genutzt werden kann.

Bevor aber mit dem ersten Schritt begonnen werden kann, müssen zunächst grundlegende Fragen beantwortet werden. Fragen wie: Was wollen wir mit unserem IT-Security-Management erreichen? Wer soll es verantworten? Wie ist die Rolle eines jeden Einzelnen?

15.5.2 Vorarbeiten

Ein ISMS-Projekt lässt sich in eine Anzahl von Meilensteinen untergliedern. Einige oder aber alle diese Meilensteine können nur abgeschlossen werden, wenn die erarbeiteten Ergebnisse durch einen Lenkungsausschuss abgenommen wurden. In Betrachtung der Tragweite ist es angemessen, wenn die Abnahme durch die Unternehmensleitung erfolgt. Dazu gehören Eckpunkte



KAPITEL 15 – PRAXIS: AUFBAU EINES ISMS

wie die allgemeine Behandlung von Risiken, also die Definition, abhängig von welchen Rahmenbedingungen Risiken getragen oder eben nicht getragen werden, oder die generellen Ziele, die die Unternehmensführung bezüglich des Informationsschutzes verwirklicht sehen möchte.

Der Fokus eines ISMS-Projekts verlässt recht schnell das Gebiet der klassischen IT und richtet sich auf Bereiche, die mit Technik im Allgemeinen nur aus Sicht eines Anwenders zu tun haben. Dazu gehören unter vielen anderen die Personalabteilung, der Einkauf, der Bereich der Produktion oder die Entwicklungsabteilung. Diese Bereiche arbeiten täglich mit IT-Gerätschaften und verarbeiten wichtige Daten, sehen die IT aber eher als Dienstleister und sich selbst selten als Dateneigentümer und damit in der Verantwortung, im Rahmen des IT-Risikomanagements Entscheidungen zu treffen, also Entscheidungen, was den Umgang mit den Daten betrifft und die Klassifizierung derselben. Der Einbezug dieser Personenkreise ist aber essenziell, da sie letzten Endes durch ihr verantwortungsbewusstes oder auch falsches Verhalten den Erfolg oder Misserfolg des Informationsschutzes mitbestimmen.

Mindestens vier Themengebiete müssen abschließend bearbeitet werden, bevor mit der Einrichtung eines ISMS begonnen werden kann. Einige dieser Punkte sind auch schon Voraussetzung für die Implementierung einer IT-Security-Organisation und sollten aus diesem Grund bereits im Unternehmen fest verankert sein. Ist dies nicht der Fall, dann gehören sie zu den ersten Maßnahmen, die es umzusetzen gilt.

Aufgabenspektrum definieren

Wie wichtig ist die IT-Security für das Unternehmen und wie passt die IT-Security-Strategie zur IT-Strategie und letzten Endes zur Unternehmensstrategie? Diese Fragen zu beantworten, steht am Anfang jeder Überlegung, die zur Ausgestaltung eines IT-Security-Managements führt. Sie legen die Bandbreite fest, in deren Rahmen gearbeitet wird, und die Intensität, mit der diese Arbeit verfolgt wird. Daraus lässt sich aber nicht nur die Strategie ableiten, sondern auch der Aufbau der IT-Security-Organisation sowie die Kompetenzen, der Geltungsbereich und die finanziellen Mittel, die für diese Aufgabe zur Verfügung stehen.

Es ist sinnvoll, an dieser Stelle bereits die Richtung anzugeben, in die ein Unternehmen sich bezüglich des Schutzes von Daten weiterentwickeln will.



Einige grundlegende Fragen können in diesem Stadium bereits beantwortet werden:

- Soll eine Zertifizierung nach ISO 27001 oder BSI stattfinden?
- Soll das IT-Risikomanagement bestimmten Normen folgen?
- Welche Vorgaben und Gesetze sind besonders wichtig im Rahmen des Projekts?
- Wie ist der Verantwortungsbereich der IT-Security-Organisation gestaltet?
- Welche Verantwortung haben die Mitarbeiter im Umgang mit Daten?

Aus den Antworten der oben aufgeführten Fragestellungen ergeben sich die IT-Security-Ziele, die wiederum die Grundlage für das IT-Security-Management darstellen. Jede Tätigkeit, jede Festlegung, jede Richtlinie und jede Entscheidung im IT-Security-Management beruht auf den Rahmenbedingungen, die durch diese Ziele definiert werden.

IT-Security-Ziele können unter anderem wie folgt aussehen:

- Einhalten der Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität auf Basis der Klassifizierung von Unternehmenswerten. Eventuell Hinzunahme des Schutzzieles »Belastbarkeit«, um den Anforderungen der EU-DSGVO zu entsprechen.
- In der Darstellung nach außen muss deutlich sein, dass der Schutz von eigenen, aber auch fremden Daten eine hohe Priorität genießt.
- Die Einhaltung gesetzlicher oder anderer Vorgaben im Rahmen der IT-Compliance wird sichergestellt.
- Ein IT-Risikomanagement gewährleistet, dass Unternehmenswerte ange messen, d.h. ihrem Wert entsprechend, geschützt werden.
- Die Erreichung der Unternehmensziele wird mithilfe der IT-Security unterstützt. Dies geschieht unter anderem durch die Sicherstellung der Kontinuität von Prozessen und Arbeitsabläufen.

Einzelne Ziele können als unterschiedlich wichtig eingestuft werden. Diese Abstufung sollte klar herausgearbeitet werden, um als Handlungsgrundlage für IT-Security-Prozesse dienen zu können.

Die Definition von IT-Security-Zielen erfolgt auf Basis der Ergebnisse von Ablaufanalysen, die aufzeigen, welche Unternehmensziele mit den IT-Zielen



KAPITEL 15 – PRAXIS: AUFBAU EINES ISMS

verknüpft sind und, davon abgeleitet, welche IT-Security-Ziele festgelegt werden müssen, um diese zu unterstützen.

Wichtig

Der Begriff »IT-Security« mit dem Präfix »IT« ist irreführend. Die Sicherheit für Unternehmensdaten liegt nicht in der originären Verantwortung der IT-Abteilung, auch wenn diese Aufgabe häufig an diese delegiert wird. Letzten Endes wird immer die Unternehmensleitung in der Pflicht stehen, für die Sicherheit der Unternehmenswerte zu sorgen.

15

Die Verantwortung der Unternehmensführung für die Zielerreichung in allen Geschäftsbereichen erstreckt sich auch auf die IT-Security, d.h. die Sicherstellung, dass Daten und Informationen, also das Know-how des Unternehmens und von Kunden und Lieferanten, nicht missbraucht wird. Die Grundlage für diese Verantwortung bilden gesetzliche Regelungen und zusätzlich dazu alle internen und externen Vereinbarungen. Daraus kann abgeleitet werden, dass es Aufgabe der Unternehmensleitung ist, das IT-Security-Management einzusetzen, zu steuern und zu überprüfen.

Die Erforderlichkeit der Kontrolle durch die oberste Leitungsebene, und damit die Gesamtverantwortung bleibt davon unberührt. Es ist wichtig, Konsens über diese Punkte zu erreichen, um die erforderliche Managementunterstützung zu erhalten. Häufig ist es angeraten, dazu externe Berater hinzuzuziehen, die sowohl die Verantwortung und damit Haftung als auch die gesetzlichen Rahmenbedingungen aufzeigen. Außerhalb der internen Hierarchie stehend, wird es einem Externen auch leichter fallen, unangenehme Wahrheiten auszusprechen und auch auf tiefgreifende Änderungen zu pochen.

Geltungsbereich

Die Beschreibung des Geltungsbereichs (*scope*), also der Anwendungsbereich des ISMS, wird festgelegt. Mit diesem Schritt werden die Grenzen des ISMS definiert. Das ist zum einen erforderlich, um bei einer Zertifizierung klar aufzuzeigen zu können, was Bestandteil der Prüfung ist und was nicht, und zum anderen wird sich der Manager IT-Security darauf berufen können, was laut Definition mit betrachtet werden muss und welche Bereiche nicht mehr in seinem Verantwortungsbereich liegen.



Diese Implikationen erfordern, dass das Dokument, das den Geltungsbereich beschreibt, von der Unternehmensleitung abgesegnet werden muss. Nicht alle Standorte eines Unternehmens oder nicht alle Tochterunternehmen müssen im gleichen Maße in das aufzubauende ISMS mit eingebunden werden. Natürlich ist es vorteilhaft, im gesamten Unternehmen das gleiche Sicherheitsniveau anzustreben, häufig ist dies aber nicht möglich oder aus Kostengründen nicht angebracht. In jedem Fall sollte bei der Festlegung der Grundsatz Beachtung finden, dass das schwächste Glied in der IT-Security-Kette das Gesamtniveau bestimmt.

Sicherheitsrichtlinie

Das Grundlagendokument zur IT-Security ist die Sicherheitsrichtlinie. Es wird viele Dokumente geben, die Unterbereiche der IT-Security beschreiben, die Maßnahmen dokumentieren oder Verfahren erläutern. Die Sicherheitsrichtlinie nimmt darunter eine Sonderstellung ein. Das Papier beschreibt auf wenigen Seiten, warum ein Unternehmen der IT-Security eine hohe Stellung einräumt und wie diese in den Rahmen der Geschäftsziele einzubinden ist. Dieses Top-Level-Dokument gilt als Grundlage für die IT-Security-Organisation und ihre Prozesse schlechthin und damit auch als Basisdokument für das ISMS-Projekt. Die Sicherheitsrichtlinie heißt auf Deutsch »IS-Politik« und dieser Name ist durchaus treffend. Dieses Dokument ist, strebt man die Zertifizierung an, essenziell und bringt weitreichende Definitionen mit über Kompetenzen wie die Erstellung und Veröffentlichung von Richtlinien.

15

Richtlinien zum IT-Risikomanagement

Das IT-Risikomanagement durchzieht alle Phasen der ISMS-Implementierung und des Betriebs. Aus diesem Grund ist es wichtig, dass die genaue Umsetzung aller einzelnen Stufen in einem Dokument beschrieben wird. Anhaltspunkte ergeben sich aus der ISO 27005 »Information technology – Security techniques – Information security risk management«.

Die Festlegung, wie mit Risiken umgegangen wird (*risk treatment*), ist gleichfalls Aufgabe des Managements. Dabei werden die Kriterien definiert, nach denen entschieden wird, ob ein Risiko getragen bzw. reduziert wird oder aber ob es ausgelagert werden muss. Diese Entscheidung basiert im Wesentlichen auf einer Risiko-Kosten-Abwägung.



KAPITEL 15 – PRAXIS: AUFBAU EINES ISMS

Die Klassifizierungsrichtlinie stellt als weitere Basisrichtlinie die Anleitung dar, wie im Rahmen des IT-Risikomanagements eine Bewertung der Unternehmenswerte und damit auch deren Behandlung auszusehen hat. Auch dieses Dokument ist ein wichtiger Eckpfeiler, der im weiteren Prozess der Ausgestaltung des ISMS vonnöten ist.

ISMS-Handbuch

Der Begriff »ISMS-Handbuch« kommt in den Normen nicht vor und beschreibt ein Dokument, das die Aufgabe wahrnimmt, die bereits erwähnten Basisrichtlinien miteinander in einen Kontext zu setzen. Es beschreibt die Aufgaben des ISMS genauso wie die Organisation der Informationssicherheit, den Zusammenhang zwischen der Erfassung von Risiken, der Klassifizierung von Daten bis hin zur Ableitung von Maßnahmen. Damit ist das ISMS-Handbuch das Dokument, das ein unbeteiligter Mitarbeiter zuerst in die Hand nimmt, um daraus alles für ihn Wissenswerte zu lernen.

15

15.5.3 Plan: Gestaltung des ISMS

Die IT-Security-Organisation steht, die Unternehmensleitung ist informiert und erteilt den Auftrag, das ISMS-Projekt zu starten. Die grundlegenden Dokumente, die die eben genannten Vorsätze auch in schriftlicher Form festlegen, wurden erstellt und entsprechend verteilt. Nun beginnt die Planungsphase des Projekts.

In dieser Phase müssen die Ansprüche der Unternehmensleitung, der IT-Security-Organisation, der IT-Abteilung und anderer beteiligter Bereiche unter einen Hut gebracht und ausformuliert werden. Auf dem Weg zu einem Projektplan müssen damit einige Fragen beantwortet werden:

- Was will das Unternehmen mit der Ausgestaltung eines ISMS erreichen?
- Wie hoch soll das allgemeine Sicherheitsniveau letztendlich werden und wie sehen die Schritte bis zum Ziel aus?
- Wo sollen die Schwerpunkte liegen?
- Wer kümmert sich um was?
- Wie soll das Projekt ablaufen und wer stellt die Ressourcen zur Verfügung?

Nur wenn die eben genannten Fragen beantwortet sind, kann eine sinnvolle Durchführung des Projekts stattfinden. Die Antworten auf die Grundsatzfragen, die im Vorfeld gegeben wurden, stellen dafür die Basis dar.



Hinweis

Die Plan-Phase ist ähnlich aufgebaut wie die Projektplanungsphase anderer größerer Projekte auch. Budgets werden festgelegt, Ressourcen zugeteilt, Zusammenhänge mit anderen Projekten aufgezeigt sowie die Projektziele definiert und mit überprüfbaren Kennzahlen unterlegt. Am Schluss der Plan-Phase existieren ein Plan mit Teilprojekten und Arbeitspaketen und ein Zeitstrahl, der den Projektablauf terminiert und die Projektplanung visualisiert.

Beginnt man auf der »grünen Wiese«, bilden sich die Strukturen einer IT-Security-Organisation also erst noch heraus, dann ist es auch nicht erforderlich, auf bestehende Prozesse und Richtlinien Rücksicht zu nehmen. In diesem Fall kann naturgemäß deutlich einfacher eine definierte Ideallinie verfolgt werden. In den allermeisten Unternehmen wird es aber bereits eine Reihe von beschriebenen Prozessen und Methoden geben, um Datensicherheit zu gewährleisten. In diesen Fällen behandelt das Projekt vorrangig die Anpassung oder Neuimplementierung von Prozessen.

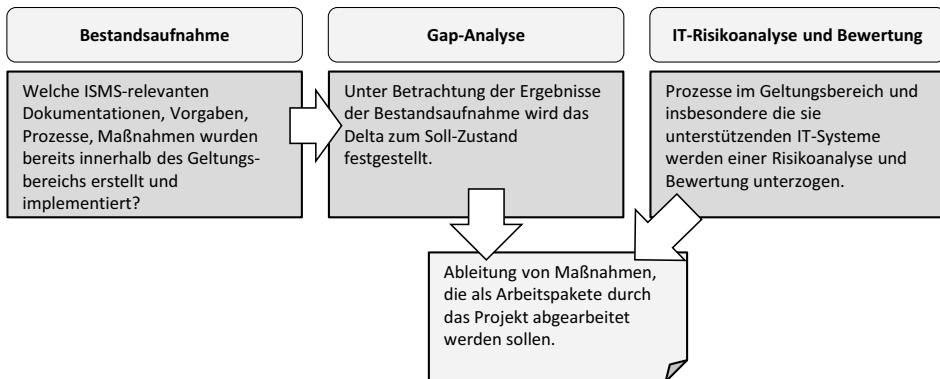
Nicht immer sind vorhandene Prozesse auf einen Blick als koordinierte IT-Security-Prozesse erkennbar. Manchmal kümmern sich Institutionen wie der Sicherheitsingenieur neben dem Zugangsschutz mithilfe von Mitarbeiterausweisen auch um den Zugangsschutz zu Computerräumen, stellt Regeln zum Umgang mit Arbeitsplatzrechnern auf oder arbeitet zusammen mit einzelnen Mitarbeitern der IT am Virenschutz. Diese oftmals seit vielen Jahren existierenden Stellen müssen ermittelt und die dort bereits erarbeiteten und gelebten Methoden ins Projekt integriert werden.

Dazu kommt, dass sich in Unternehmen, in denen IT-Security keiner einzelnen Abteilung zugeordnet wurde, häufig an den unterschiedlichsten Stellen Mitarbeiter finden, die sich sehr wohl Gedanken darüber machen, wie sie ihre Arbeit auch unter dem Aspekt Datensicherheit gestalten können. Diese Arbeit verrichten sie ohne formale Grundlagen, aber gerade deshalb auch häufig hoch integriert und hocheffizient. Ein Beispiel ist oftmals in der sogenannten »Schatten-IT« zu finden – also in Bereichen wie der Produktion. Die meisten größeren Maschinen sind seit geraumer Zeit mit eigenen Computern ausgerüstet, die entweder fest in der Maschine verbaut oder direkt mit ihr verbunden sind. Dazu kommt, dass seit Industrie 3.0 Maschinen mit Maschi-



KAPITEL 15 – PRAXIS: AUFBAU EINES ISMS

nen »sprechen« und dies geschieht regelmäßig über das Unternehmensnetzwerk. Dabei sind die genutzten Protokolle entweder vergleichbar mit denen der »regulären« Clients und Server oder aber unterscheiden sich grundlegend. Für jede dieser Maschinen wird es einen Betreiber geben und dieser wird in den seltensten Fällen in der IT-Abteilung zu finden sein.



15

Abbildung 15.5: Wesentliche Aufgaben der Plan-Phase

Informationen über bereits existierende Sicherheitsprozesse und das Wissen und die Erfahrungen der Mitarbeiter müssen zusammengetragen und ausgewertet werden, weil sie einen gewissen Einfluss auf die Projektplanung haben. Wird z.B. der Informationsschutz für Personaldaten bereits durch eine eigene Abteilung verantwortet, die in der Personalabteilung angesiedelt ist, dann wird keine Neuplanung, sondern eine Integration in das neue ISMS erforderlich sein. Unter Umständen können aus der Arbeit, die in dieser Abteilung geleistet wird, auch wertvolle Hinweise abgeleitet werden.

Die Vorgehensweise der Plan-Phase, wie sie in Abbildung 15.5 dargestellt ist, lässt sich grob in die folgenden Unterphasen gliedern:

- Eine **Bestandsaufnahme** zeigt auf, wie das Unternehmen bezüglich der IT-Security aktuell aufgestellt ist, und deckt bereits vorhandenes Wissen auf. Auch wenn der Bereich, der später durch das ISMS abgedeckt werden soll, kleiner sein wird, ist es dennoch sinnvoll, alle im Unternehmen implementierten Prozesse und Dokumentationen zu sichten.
- Die **Gap-Analyse** gleicht den Ist-Zustand mit dem Soll-Zustand ab.
- Die **Risikoanalyse und Risikobewertung** identifiziert die zu schützenden Unternehmenswerte und ermittelt die jeweils bestehenden Bedrohungen.



Aus den Bedrohungen und deren Eintrittswahrscheinlichkeiten werden Risiken abgeleitet, beschrieben und bewertet. Aus der Aufstellung der Unternehmenswerte, deren Klassifizierung und den jeweiligen Risiken werden **Maßnahmen** abgeleitet und deren Implementierung geplant.

Hinweis

In der ISO 27001 aus dem Jahr 2005 stand der Unternehmenswert im Mittelpunkt. Damit war vorgegeben, dass zunächst alle Werte zu ermitteln sind, bevor jeweils die Schwachstellen, Bedrohungen und letzten Endes das jeweilige Risiko definiert wurden. Diese Vorgehensweise hat sich als suboptimal herausgestellt, da die Anzahl der Werte je nach Herangehensweise unüberschaubar groß geworden ist. Da aber letzten Endes das Risiko im Fokus der Bemühungen steht, wurde in der ISO 27001 der Version 2013 ein Schwenk vollzogen, der das Risiko nun in das Rampenlicht rückt. Primär ist nun das Risiko zu identifizieren und die davon betroffenen Unternehmenswerte sind diesem zuzuordnen. Die darauf folgende Vorgehensweise ändert sich indes nicht – das Werkzeug IT-Risikomanagement gewinnt allerdings weiter an Gewicht.

15

Der Umfang der Arbeitspakete wird aus den offenen Punkten der Gap-Analyse und den Ergebnissen der Risikoanalyse ermittelt. Die Gap-Analyse wird eher die Erstellung von Dokumenten wie Regelungen oder Prozessbeschreibungen zur Folge haben, während aus der Risikoanalyse neben Prozessanpassungen auch technische Maßnahmen abgeleitet werden. Alle Aufgaben werden zu **Teilprojekten und Arbeitspaketen** des Projekts.

Bestandsaufnahme

Die Feststellung der aktuellen Situation ist der erste Schritt in der Plan-Phase. Nicht nur für das Management und die Sponsoren des Projekts, sondern auch für das Projektteam ist es wichtig, zu wissen, wo man steht, um daraus ableiten zu können, welcher Weg noch vor einem liegt. Um dabei die eben erwähnten unterschiedlichen Personenkreise zu erreichen, ist eine ausführliche Vorbereitung erforderlich. Auch werden an die Bestandsaufnahme und die Auswertung der Ergebnisse hohe Anforderungen gestellt.

**Tipp**

Die Bestandsaufnahme kann abhängig von der Größe und Komplexität des Geltungsbereichs und der Qualität der vorhandenen Dokumente oft in wenigen Tagen abgehandelt werden. Dieser Teil ist häufig auch in einem Vorprojekt zu finden und dient, zusammen mit den Ergebnissen der Risikoanalyse der allgemeinen Übersicht, der Managementpräsentation und als Grundlage für die Kostenabschätzung des Projekts.

15

In Unternehmen, die keine ganzheitliche Herangehensweise verfolgen, kann die Bestandsaufnahme durchaus auf vereinzelte Bereiche angewandt werden, die unter Umständen kaum Kontakt zueinander haben. Dies kann z.B. dann der Fall sein, wenn neben der IT und der Personalabteilung auch noch gezielt ein Entwicklungsbereich in einem Tochterunternehmen mit einbezogen werden soll. In diesem Fall könnte man zwei oder auch drei eigene und unabhängige Bestandsaufnahmen anfertigen. Am Schluss werden diese aber wieder zusammengeführt werden müssen, um Redundanzen in Maßnahmen und dem IT-Risikomanagement zu vermeiden.

Sehr häufig wird es bereits Ergebnisse aus zurückliegenden Betrachtungen oder sogar eine organisierte Sammlung von vorhandenem Material im Unternehmen geben. Diese werden vielleicht nicht der in diesem Projekt zugrunde gelegten Norm entsprechen, nichtsdestotrotz können die bereits erfassten Dokumente die jetzt durchgeföhrte Aufnahme deutlich beschleunigen.

Für den Fall, dass in der Vergangenheit noch keine Aufnahme stattgefunden hat oder falls die letzte Sammlung von Dokumenten etc. zu weit in der Vergangenheit liegt, wird es schwerer, geeignetes Ausgangsmaterial zu erhalten. In diesen Fällen ist es umso sinnvoller, die Strukturierung von neuen, aber auch alten Materialien z.B. direkt an den Maßnahmzielen auszurichten.

Für den Vorgang der Pflege der Dokumente, die im Rahmen der Bestandsaufnahme gesammelt oder neu erstellt werden, gilt ganz besonders, dass ein Inventar nur so gut ist wie die Prozesse, die dazu eingesetzt wurden, dieses aktuell zu halten. Dabei reicht es im Allgemeinen nicht aus, eine jährlich aktualisierte Version zu veröffentlichen. Es ist eher anzustreben, automatisierte Vorgänge zu implementieren, um diese Listen auf dem Laufenden zu halten. Für Bereiche, in denen dennoch manuelle Eingriffe erforderlich sind,



müssen dementsprechende Richtlinien bestehen, wann und wie und von wem Listen gepflegt werden müssen.

Grundsätzlich lohnt es sich, in verschiedenen Bereichen des Unternehmens, auch jenseits der IT, nachzuforschen. Dazu gehören auch diverse Fachabteilungen wie Entwicklungsabteilungen, Logistik und die Personalabteilung. Letztendlich hat sich aber immer wieder gezeigt, dass die wesentlichen IT-Security-Prozesse in den Bereichen vorhanden sind, die sich hauptsächlich mit dem Betrieb der IT-Systeme befassen.

Gap-Analyse

Die Gap-Analyse dient der Ermittlung des Deltas zwischen den Anforderungen an das Ergebnis des ISMS-Projekts und den Erkenntnissen aus der Bestandsaufnahme. Also der Vergleich mit den bereits bestehenden Prozessen, Methoden, dem Wissen bei Mitarbeitern und dem, was bereits in Dokumenten niedergeschrieben wurde. Es geht dabei nicht nur um eine Sammlung aller Dokumente, sondern genauso darum, herauszufinden, wie bislang mit Risiken und Daten umgegangen wurde, um davon abzuleiten, welche Schwerpunkte im ISMS-Projekt gesetzt werden müssen.

15

Hinweis

Es ist an diesem Punkt des Projekts oft nicht möglich, eine vollständige Liste mit allen offenen Punkten zu erstellen. Viele Einzelheiten werden erst im Laufe des Projekts ermittelt werden. Auf der anderen Seite sollte es aber zumindest möglich sein, wenigstens auf einer groben Ebene in Erfahrung zu bringen, welche Themen bislang sehr gut oder eben mangels bearbeitet wurden und in welchem Gebiet beschriebene Prozesse und Dokumentationen existieren bzw. in welchen nicht.

Grundlage für eine Gap-Analyse ist immer eine Liste, die aufzeigt, was bereits vorhanden sein sollte. Anhand dieser Liste wird im Rahmen der Bestandsaufnahme und mithilfe zusätzlicher Maßnahmen wie z.B. durch Interviews festgestellt, welche Punkte noch offen und welche bereits ausreichend umgesetzt sind. Damit steht und fällt die Qualität einer Gap-Analyse mit der Qualität dieser Liste. Es ist zu empfehlen, entweder auf vorhandene Listen von Experten zuzugreifen oder sich zumindest am Rahmen des Anhangs A der ISO 27001



KAPITEL 15 – PRAXIS: AUFBAU EINES ISMS

oder der ISO 27002 zu orientieren. Der Anhang A formuliert Themenbereiche, Maßnahmenziele und Maßnahmen, die für die IT-Security von Bedeutung sind. Ausgehend von diesen Vorgaben fällt es leichter, eigene Punkte zu erstellen und hinzufügen.

Eine Gap-Tabelle kann damit aussehen wie nachfolgend fragmentarisch dargestellt. Die Maßnahme in der ersten Spalte bezieht sich jeweils auf eine Maßnahme aus Anhang A der ISO 27001.

Maßnahme	Frage	Auswertungskriterien	Bewertung
A.5 Sicherheitsleitlinie	Basisrichtlinien sind vorhanden und mit der Unternehmensleitung abgestimmt: Sicherheitsrichtlinie, Klassifizierungsrichtlinie, Richtlinie zum IT-Risikomanagement	Umsetzungsgrad: None: Keine Richtlinien vorhanden Partially: Nur Sicherheitsrichtlinie vorhanden Largely: Sicherheitsrichtlinie und Klassifizierungsrichtlinie vorhanden Fully: Alle Richtlinien vorhanden und umgesetzt	
A.6 Organisation der Informationssicherheit	Die Informations-sicherheitsorganisation ist etabliert, mit Ressourcen und Kompetenzen ausgestattet.	None Partially Largely Fully	
A.7 Personal-sicherheit	Prozess ist vorhanden und beschrieben, der die IT-Abteilung unterrichtet, wenn ein Mitarbeiter die Firma verlässt.	None Partially Largely Fully	
	Prozess ist vorhanden und beschrieben, der dafür Sorge trägt, dass ausscheidende Mitarbeiter alle Gerätschaften geordnet zurückgeben.	None Partially Largely Fully	



Neben den Fragen und Antworten ist es wichtig, folgende Details zu dokumentieren:

- Interviewpartner
- Funktion des Interviewpartners
- Bereich, für den das Interview geführt wurde
- Datum
- Version

Diese Zusatzdaten dienen vor allem der Wiederholbarkeit der Gap-Analyse. So kann es durchaus sinnvoll sein, dass während des Projekts wiederholt eine Gap-Analyse durchgeführt wird, um Fortschritte zu dokumentieren. Dies fällt so oft einfacher, als sie aus einem laufenden, großen ISMS-Projekt zu extrahieren.

Für den späteren Projektverlauf dienen die ausgefüllten Formulare der Gap-Analyse dazu, den jeweiligen Ansprechpartner für jeden Bereich zu identifizieren und dort verzeichnete Links zu Dokumenten direkt nutzen zu können. Im Grunde handelt es sich also um eine erste Übersicht mit vielen Hinweisen und Hilfen für den weiteren Projektverlauf.

Auswertung und Darstellung der Ergebnisse der Gap-Analyse

Die Gap-Analyse folgt den Schritten zur Implementierung eines ISMS und fragt allerhand Teilbereiche ab, die einer vorgefertigten Liste entnommen sind. In diesem Beispiel wird davon ausgegangen, dass der Anhang A der ISO 27001 und die ISO 27002 die Basis für eine Anforderungsliste bilden. Angenommen, der jeweilige Umsetzungsgrad wurde stufenweise bewertet, so sollten nun für jedes Teilgebiet Daten vorliegen.

Bei standardisierten Bewertungskriterien können diesen Parameter zugeordnet werden, die es letztendlich ermöglichen, eine quantifizierte Bewertung des Umsetzungsgrades anzugeben. Ein Beispiel für eine solche Zuordnung, abgeleitet vom Reifegradmodell der ISO 15504, könnte folgendermaßen aussehen:

- *None* (keine Umsetzung): 0–15 Punkte
- *Partially* (teilweise umgesetzt): 16–50 Punkte
- *Largely* (weitgehend umgesetzt): 51–85 Punkte
- *Fully* (vollständig umgesetzt): 86–100 Punkte



Werden die Antworten ausgewertet, können die Ergebnisse in einem Chart dargestellt werden, das auch den Projektfortschritt dokumentiert.

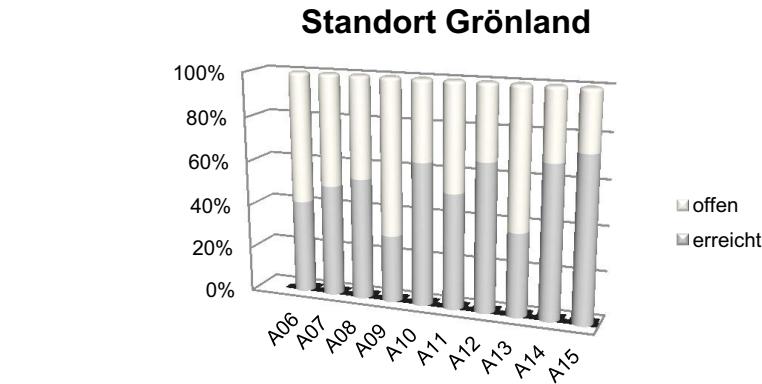


Abbildung 15.6: Mögliche standardisierte Wiedergabe der Ergebnisse einer Gap-Analyse auf Basis der Maßnahmenziele der ISO 27001

In Abbildung 15.6 ist eine solche Darstellung enthalten. Liegt eine solche für jeden einzelnen Standort vor, so können auf einen Blick die wichtigsten Aufgabenfelder identifiziert werden, auf die man sich auch zuerst konzentrieren sollte. Außerdem ist der Vergleich zwischen verschiedenen Standorten oder Töchtern eines Unternehmens möglich.

Teilprojekte und Arbeitspakete

Die Gap-Analyse ist ein wichtiger Schritt, um zu erfahren, was in welchen Bereichen noch offen ist. Diese Informationen liegen nun vor. Das bedeutet im Normalfall einen großen Stapel an Dokumenten, Prozessbeschreibungen und beschriebenen Methoden – also alles, was dem IT-Security-Management in irgendeiner Form zugeordnet werden kann.

Eine Strukturierung der Teilprojekte und Arbeitspakete kann nun auf vielfältigste Weise stattfinden. Ein häufiger Ansatz verfolgt die Gliederung auf Basis der Maßnahmenziele des Anhangs A der ISO 27001, der wie folgt aussehen könnte (siehe auch Abbildung 15.7):

- Richtlinien
 - Basisrichtlinien (Sicherheitsrichtlinie, Klassifizierungsrichtlinie, Richtlinie zum IT-Risikomanagement)



- IT-Richtlinien
- Allgemeine Richtlinien für den Umgang mit Daten, Internet, E-Mail, Gerätschaften und Passwörtern



15

Abbildung 15.7: Übersicht über die verschiedenen Maßnahmenziele der ISO 27001

- IT-Security-Organisation
 - Einbindung Unternehmensleitung und Schaffung entsprechender Kommunikationskanäle
 - Aufbau der IT-Security-Organisation und Definition von Rechten und Pflichten
- Management von Unternehmenswerten (*assets*)
 - Aufbau eines Assetmanagements
 - Klassifizierung von Unternehmenswerten
- IT-Risikomanagement
 - Implementierung von Software zur Unterstützung der Identifizierung, Bewertung und Behandlung von Risiken
 - Beschreibung der Vorgehensweise von Risikoanalyse, Risikobewertung und Risikobehandlung



KAPITEL 15 – PRAXIS: AUFBAU EINES ISMS

■ Personalsicherheit

- Prozesse für den Umgang mit neuen Mitarbeitern
- Prozesse für den Umgang mit Berechtigungsänderungen während der Anstellung
- Prozesse zur Aufhebung von Zugriffsrechten nach der Einstellung

■ Infrastrukturelle Sicherheit

- Sicherung der Infrastruktur (z.B. Rechenzentrum, Büros)
- Sicherheit von Gerätschaften

■ Betrieb

- Dokumentation von Prozessen
- Dokumentation von IT-Systemen
- Maßnahmen für den sicheren Zugriff auf Daten
- Schutz vor Schadsoftware, Patchmanagement
- Vorgaben für die Datensicherung
- Netzwerksicherheit
- Umgang mit Speichermedien
- Richtlinien zur Übermittlung von Daten
- Monitoring, Zugriffsprotokollierung und Auditierung

■ Zugangskontrolle

- Richtlinien zum Zugangsschutz zu Gebäuden
- Benutzerverwaltung (*identity management*)
- Verantwortung jedes Benutzers zum Schutz von Informationen
- Zugangskontrolle für das Netzwerk
- Zugriffskontrolle auf Betriebssysteme und Anwendungen

■ Beschaffung, Entwicklung und Wartung von Informationssystemen

- Festlegung von Spezifikationen von Hard- und Software
- Prozesse zum Schutz der Integrität von Daten bei und nach der Eingabe in Applikationen



- Maßnahmen zur Verschlüsselung
- Dokumentation von Änderungen an Hard- und Software
- Umgang mit Sicherheitsvorfällen
 - Prozesse zur Meldung und Abarbeitung von Sicherheitsvorfällen
 - Richtlinien zur IT-Forensik
- IT Business Continuity Management
 - Anforderungen aus dem Bereich IT-Compliance
 - Umsetzung eines IT-Notfallmanagements
 - Technische Maßnahmen zur Fortführung des Geschäftsbetriebs

Auch eine organisatorische Gliederung nach IT-Abteilung, Personalabteilung, Datenschutz und weiteren betroffenen Einheiten ist denkbar. Unter IT-Abteilung können dann Abteilungen und Anlagen wie das Rechenzentrum angeordnet werden.

Die letzte Ebene ist die der Arbeitspakete. Auf diesen werden die einzelnen Maßnahmen festgelegt.

Risikoanalyse und Risikobewertung

Die Gap-Analyse hat ergeben, welche offenen Baustellen es von einer erhöhten Sicht aus gibt. Ein Abgleich mit entsprechenden Maßnahmenlisten stellt sicher, dass keine Bereiche übersehen werden. Der nun anstehende Schritt fügt den offenen Punkten die deutlich detailliertere Sicht auf die einzelnen Unternehmenswerte hinzu. Ging es bislang eher um Prozesse und deren Dokumentationen, so werden nun die Sicht auf Risiken und die Ableitung entsprechender Maßnahmen hinzugefügt.

Dafür sind zunächst die bestehenden Risiken und die davon betroffenen IT-Systeme, Daten und Applikationen zu identifizieren. Dabei konzentriert man sich auf diejenigen Unternehmenswerte, die im Geltungsbereich liegen. Diese Informationen können relativ leicht aus den Interviews, den Prozessbeschreibungen und den anderen Informationen, die im Rahmen der Gap-Analyse gesammelt wurden, abgeleitet werden.

**Tipp**

Der Ansatz, mit der Risikoanalyse bei den fünf wichtigsten Geschäftsprozessen zu beginnen, hat sich bewährt. Werden diese abgearbeitet und die jeweiligen darunter liegenden IT-Systeme und Daten einer Risikoanalyse und Risikobewertung unterzogen, so ist häufig bereits ein Großteil aller wichtigen IT-Systeme abgedeckt.

15

Liegen bereits die Ergebnisse einer Business-Impact-Analyse (BIA) vor, dann können die identifizierten Unternehmenswerte direkt priorisiert werden. Sind diese nicht vorhanden, dann kann es Sinn machen, dies nun nachzuholen. Die Abarbeitung der Risiken erfolgt dabei nach ihrer in der BIA ermittelten Priorität. Damit wird die Grundlage geschaffen, um daraus technische Maßnahmen, Richtlinien, Prozessanpassungen oder andere Tätigkeiten aus dem Werkzeugkasten der IT-Security-Organisation abzuleiten.

Die wesentlichen Mechanismen, die dabei Verwendung finden, werden in den Kapiteln zum IT-Risikomanagement und zum IT-Notfallmanagement ausführlicher beschrieben. Zusammengefasst kann es folgendermaßen ausgedrückt werden: Die Business-Impact-Analyse ermittelt die wirklich kritischen Unternehmenswerte, das IT-Risikomanagement ermittelt den aktuellen Gefährdungsstand und bildet die Grundlage für die daraus abzuleitenden Maßnahmen.

Alle Maßnahmen sollten einem einheitlichen Maßnahmenkatalog entstammen, der im besten Fall im gesamten Unternehmen herangezogen und deshalb auch zentral gepflegt wird. Das macht Ergänzungen und Anpassung an den technischen Fortschritt deutlich einfacher und effektiver. Außerdem ist es nur so möglich, den Überblick zu bewahren, insbesondere wenn man über Hunderte von Maßnahmen spricht, die Dutzenden von Richtlinien folgen.

Hinweis

Die Zuteilung von Personen zu Arbeitspaketen ist ein relativ einfacher Schritt, die Abschätzung der internen und externen Kosten ist dagegen wie in jedem komplexen Projekt eine größere Herausforderung. Findet diese Festlegung im Anschluss einer Gap-Analyse statt, dann wird diese



Schätzung treffsicherer sein, als fände eine Schätzung ohne diese Grundlage statt.

Innerhalb der Projektplanung werden Fragen nach der Verhältnismäßigkeit von Maßnahmen und nach der Verantwortlichkeit laufend im Mittelpunkt stehen. Das hat vor allem damit zu tun, dass in dieser Phase der Umfang des Projekts vollständig offenbart wird und damit Abhängigkeiten sichtbar werden, die zuvor eventuell nicht gesehen wurden. Da ist es nur natürlich, dass Punkte, die zuvor als erforderlich erachtet wurden, nun erneut auf dem Prüfstand stehen.

Die Messlatte für Entscheidungen für und wider die Maßnahmen kann letztendlich nur durch die Unternehmensleitung bzw. den Lenkungsausschuss des Projekts getroffen werden und muss daher von den Basisdokumenten abgeleitet werden. Im Rahmen der dort aufgeführten grundsätzlichen Festlegungen muss der jeweilige Dateneigentümer die Verantwortung schultern, Aussagen über die Klassifizierung von Daten und IT-Systemen vorzunehmen, und damit mit über die Art und den Umfang davon abgeleiteter Maßnahmen bestimmen.

Die IT-Security baut naturgemäß weitgehend auf der eingesetzten IT-Infrastruktur und IT-Systemen auf. In heterogenen Umgebungen können diese von Abteilung zu Abteilung und Prozess zu Prozess stark variieren. Es ist deshalb sehr selten möglich, anhand eines »Standardsystems« generelle Vorgehensweisen abzuleiten. Vielmehr sind individuelle Eigenarten und Abweichungen zu berücksichtigen.

Hinweis

Die Festlegung von Maßnahmen und die Gründe dafür und auch Gründe, warum in einem Fall auf eine Maßnahme verzichtet wird, sollten Eingang in die Dokumentation des ISMS finden.

Zusätzlich zu den technischen Informationen müssen die Anforderungen aus der IT-Compliance mit den tatsächlich existierenden Gegebenheiten abgeglichen werden. Daraus entsteht wiederum eine Liste mit eventuellen Lücken in der ordnungsgemäßen Umsetzung. Diese Liste ist parallel zu den



KAPITEL 15 – PRAXIS: AUFBAU EINES ISMS

Ergebnissen der technischen Erfassung zu sehen und auch weitgehend parallel abzuarbeiten.

Die nachfolgenden Punkte können als Richtschnur dienen, welche Bereiche nach kritischen Werten abgesucht werden sollten, bevor diese dann näher durch das IT-Risikomanagement untersucht werden.

Komplexe Systeme

In einem ersten Schritt ist es sinnvoll, strategisch eingesetzte, komplexe Technologien zu erfassen. Diese bilden neben einzelnen IT-Systemen und Infrastrukturkomponenten weitere wichtige Unternehmenswerte, die spezielles Augenmerk verdienen. Grundsätzlich kann gesagt werden, dass es oftmals nicht ausreicht, vereinzelte IT-Systeme zu betrachten. Mehrere verknüpfte Systeme bilden zusammen ein übergeordnetes komplexes System, an das unter Umständen völlig andere Anforderungen gestellt werden müssen.

Zu den klassischen strategischen Technologien gehören z.B. der Zugang zum Internet, das Cloud Computing, die Datensicherungssysteme oder virtualisierte Umgebungen. Jede dieser Technologien basiert wiederum auf einer Vielzahl einzelner IT-Systeme, aber auch auf Prozessen sowie speziellen Regelungen hinsichtlich der IT-Compliance und beherbergt damit auch weitergehende Risiken, die, abgehoben von der reinen Technik, existieren und betrachtet werden müssen.

IT-Infrastruktur

Die IT-Infrastruktur besteht aus allen Systemen, die unterstützenden Charakter haben. Prominente Beispiele sind Netzwerkkomponenten, die Verkabelung, Server, Räumlichkeiten, in denen IT-Systeme betrieben werden, oder auch Dienste wie ein DNS-Dienst oder die Hard- und Software, die den Zugriff auf das Internet ermöglicht.

Diese Infrastrukturkomponenten können in Form von grafischen Darstellungen und Listen der Unternehmenswerte beschrieben werden. Die Darstellung, z.B. in Form von Netzplänen, ist dann sinnvoll, wenn Abhängigkeiten dargestellt werden müssen.

Die Erfassung von vernetzten IT-Systemen und ihre Abhängigkeiten gehört zu den anspruchsvoller Themen, wenn es um die Dokumentation geht.



Auch hier empfiehlt es sich, einen Überblick zu schaffen, der die folgenden Fragen beantworten kann:

- Was passiert, wenn eine bestimmte Infrastrukturkomponente ausfällt?
- Von welchen Komponenten sind die kritischen Geschäftsprozesse abhängig?

Arbeitsplatzrechner und Software

Innerhalb von IT-Strukturen bilden die Computer der Anwender und die darauf installierte Software die flexibelsten, heterogensten und den meisten Änderungen unterworfenen Komponenten. Sehr unterschiedliche Anforderungen von Personen, die höchst unterschiedliche Aufgaben zu bewältigen haben, bewirken ein grundsätzlich sehr inhomogenes Umfeld, was diese Gerätschaften und vor allem die installierte Softwarebasis angeht. Dies kann durch die Wegnahme lokaler administrativer Rechte und den Einsatz einer Softwareverteilungslösung weitgehend kontrolliert und standardisiert werden, aber dennoch ist hier mit die größte Gefahr für das Entstehen sicherheitsrelevanter Ereignisse zu sehen. Aus diesem Grund sind Arbeitsplatzrechner und die darauf implementierten Sicherheitsmaßnahmen wie VirensScanner, Patchmanagement und Personal Firewalls ein wichtiges Gebiet, das im Rahmen der Bestandsaufnahme und Risikobewertung untersucht werden sollte.

Die Erfassung installierter Software, das Assetmanagement, die Überwachung von Aktivitäten auf der Netzwerkseite durch IDS-Systeme oder die laufende Überprüfung auf aktuelle Softwareversionen bilden die Grundlage für die Dokumentierung dieser Geräte. Dazu kommen alle Rechner, die sich von außen in das Unternehmensnetzwerk einwählen können, und alle weiteren an das Netzwerk angeschlossenen Gerätschaften wie z.B. Drucker, IP-Telefone, Tablets, Mobiltelefone oder WLAN-Komponenten.

15.5.4 Do: Umsetzung der Arbeitspakete

Mit der Do-Phase beginnt die Umsetzungsphase des Projekts. Die Ergebnisse aus der Gap-Analyse und des IT-Risikomanagements sind in die Projektplanung eingeflossen, Teilprojekte wurden erstellt, Arbeitspakete definiert und entsprechende Ressourcen zugewiesen. Unter Kontrolle der Projektleitung wird nun entsprechend dem Projektplan die Umsetzung starten. Hat bereits im Vorfeld ein ISMS existiert, dann ändert dies nichts an der Vorgehensweise,



KAPITEL 15 – PRAXIS: AUFBAU EINES ISMS

lediglich die Anzahl der Arbeitspakete ist kleiner oder deren Umfang geringer und damit auch der Aufwand. Außerdem wird es sich in diesem Fall eher um Änderungen und Anpassungen im Umfeld existierender Prozesse handeln.

Hinweis

Die Arbeitspakete aus der Projektplanung beinhalten keine Umsetzungsanleitung und auch keine Parameter, um deren Wirksamkeit zu überprüfen. Diese Aufgaben müssen nun in der Do-Phase umgesetzt werden.

15

Die ersten Arbeitspakete, die umgesetzt werden müssen, betreffen die Unternehmensleitung: Zunächst muss der Projektplan als solcher abgesegnet werden. Dazu gehören auch die Ressourcenplanung, die Meilensteine und die Kostenschätzung. Zudem muss eine Bewertung vorgenommen werden, ob die geplanten Aktivitäten die Erreichung der gesetzten Ziele ermöglichen. Die Weiterführung des Projekts ohne Akzeptanz vonseiten der Unternehmensleitung ist keine Option.

Wird der Projektplan akzeptiert, dann sind die Abnahme der Sicherheitsrichtlinie, der Richtlinie zum IT-Risikomanagement und der Klassifizierungsrichtlinie die nächsten Aufgaben der Unternehmensleitung. Zusammen mit dem Projektauftrag als solchem legitimiert die Freigabe dieser Dokumente nicht nur die IT-Security-Organisation und das Projekt, sondern bildet das Fundament für den gesamten PDCA-Kreislauf – insbesondere auch, und das ist entscheidend, für die Zeit nach dem Projekt.

Sind diese Punkte abgearbeitet, dann folgt die systematische Abarbeitung der in der Plan-Phase definierten Arbeitspakete.

Das einwandfreie und im Rahmen der Sicherheitsparameter erfolgende Funktionieren von Prozessen und letztendlich von IT-Systemen ist das Ziel, das durch die Umsetzung von Maßnahmen erreicht werden soll. Der Verbesserungszyklus hat zudem aber auch die essenzielle Aufgabe, den Betrieb dieser Maßnahmen zu überprüfen. Neben der Implementierung von Maßnahmen sollte man sich also auch immer darum Gedanken machen, wie das Ganze im täglichen Betrieb überprüft werden kann, wie es also um die Wirksamkeit bestellt ist. Die Implementierung eines entsprechenden Monitorings ist damit auch Teil dieses Projektschritts. Dies ist natürlich nicht für jede ein-



zelle Maßnahme möglich, und deshalb ist es sinnvoll, mithilfe von Kennzahlen das Ergebnis ganzer Prozesse zu hinterfragen. Dazu können Kennzahlen gehören wie die Anzahl an entdeckten Viren an verschiedenen Stellen in der Mailkette. Damit abstrahiert man von der Maßnahme »Installation VirensScanner« hin zur Ermittlung von Zahlen, die die Auswirkungen an zentralen Punkten überwachen. Reicht dies nicht aus, dann kann durch ein Scannen der Arbeitsplatzrechner zusätzlich die Umsetzung der Maßnahme überprüft werden.

Neue Prozesse und geänderte Arbeitsschritte sind die natürliche Folge von Projekten, die derart tief in IT-gestützte Prozesse hineingreifen. Das betrifft nicht nur die IT-Abteilung, sondern durchaus auch große Teile des gesamten Unternehmens auf die eine oder andere Art und Weise. Abhängig vom Grad der Änderungen ist es angebracht, verschiedene Formen von Awareness-Maßnahmen und Schulungen anzubieten, um zum einen die Scheu vor den Änderungen zu reduzieren und zum anderen die weitreichende Unterstützung für das Projekt zu gewinnen. Diese Maßnahmen sind ein integraler Bestandteil des Projekts und Bestandteil der Do-Phase.

15

15.5.5 Check: Überprüfung des ISMS

Die Check-Phase dient der Überprüfung installierter Maßnahmen, von Dokumenten und von Prozessen. Dieser Schritt macht aus einer seriellen Vorgehensweise einen Kreislauf und bestimmt damit im Wesentlichen den PDCA-Zyklus. Innerhalb des ISMS-Betriebs kommt diesem Schritt die Aufgabe zu, regelmäßig in festgelegten Intervallen die Bestandteile des ISMS zu testen, Audits durchzuführen und Erkenntnisse aus dem Monitoring auszuwerten.

Hinweis

Für die Überprüfung und Verbesserung des ISMS ist jeweils auch der Prozessschritt »Abnahme durch das Management« vorgesehen. Ziel der Delegierung von Kontrollaufgaben an das Management ist es, das ISMS angepasst an die Unternehmensziele zu betreiben und nicht zuletzt das Bewusstsein für den Schutz von Informationen durch alle Führungshierarchien hindurch zu stärken.



KAPITEL 15 – PRAXIS: AUFBAU EINES ISMS

Im Rahmen des Projekts der Einführung eines ISMS werden zu diesem Zeitpunkt die Fäden der einzelnen Teilprojekte und Arbeitspakete miteinander verbunden und das Gesamtkonstrukt auf Wirksamkeit überprüft. So sind Prozesse wie z.B. das Umgehen mit Sicherheitsvorfällen (*incident management*) oder das Installieren des IT-Notfallmanagements zunächst eine theoretische Angelegenheit. Wenn also möglich, dann sollten sie bereits innerhalb des Projekts auch getestet werden. Zu diesem Zeitpunkt sind Anpassungen noch relativ leicht möglich.

15.5.6 Act: Umsetzung von erkannten Defiziten

Die Act-Phase nimmt das Verbesserungspotenzial auf, das in der Check-Phase identifiziert wurde, und setzt es um. Diese Phase steht also generell dafür, das ISMS zu korrigieren und zu erweitern und damit zu verbessern. Das reicht vom Reagieren auf aufgedeckte Lücken in den Notfallplänen bis hin zu Ergänzungen in Richtlinien aufgrund von Sicherheitsvorfällen, die bereits mit Mitteln der IT-Forensik untersucht wurden.

Nach der Act-Phase wird sich das Rad erneut in Bewegung setzen und mit der Plan-Phase neu beginnen. Alle Aufgaben, die in der Check-Phase erkannt und nicht in der Act-Phase implementiert wurden (die Gründe können von unzureichenden Ausgangsinformationen bis hin zu Kosten reichen, die außerhalb des Rahmens liegen), werden in der Plan-Phase erneut aufgenommen sowie eventuell neu definiert, um sie dann in der Do-Phase umzusetzen.

15.5.7 Dokumentation

Die Dokumentation spielt beim Betrieb eines ISMS eine zentrale Rolle. Es existieren keine Vorgaben, in welcher Art und Weise die Dokumentation stattfinden soll, und dementsprechend reicht sie von Notizzetteln über Excel-Listen bis hin zu datenbankgestützten Dokumentenmanagementsystemen. Trotz oder eben weil Vorgaben und Hilfestellungen durch Best Practices fehlen, muss man sich im Rahmen eines ISMS-Projekts einige Gedanken über die eingesetzten Hilfsmittel machen. Entschieden werden muss, was dokumentiert werden soll, wie dies geschehen soll, wie diese Informationen auf dem Laufenden gehalten werden und in welcher Form sie anderen zur Verfügung gestellt wird.

**Tipp**

Folgt man im Unternehmen bereits den Vorgaben der Standards ISO 9000 oder ISO 14000 und hat dementsprechende Prozesse zur Dokumentation in Betrieb, so ist man oftmals bereits auf der sicheren Seite, wenn man die diesbezüglich aufgestellten Regeln und Prozesse auch für die ISMS-Dokumentation anwendet.

Das Ziel der Dokumentation ist es, Entscheidungen nachvollziehbar zu machen, Regelungen zu erarbeiten und diese auch bekannt zu machen und darüber hinaus alles schriftlich zu erfassen, was dabei helfen kann, definierte Schutzziele zu erreichen.

Bezogen auf die Abbildung von Entscheidungsprozessen werden alle Ergebnisse und Wege der Entscheidungsfindung für jeden Einzelbereich dokumentiert, also: Jeder Themenbereich der IT-Security verfügt immer auch über eine Dokumentationskomponente. Die Kunst, darüber nicht den Überblick zu verlieren, liegt darin, jede Dokumentation immer mit dem zugrunde liegenden Unternehmenswert, Prozess oder Risiko zu verknüpfen.

15

Unternehmenswert	Dokumentiert werden muss	Lenkung
Firewall	Änderungen am Regelwerk aufgrund allgemeiner technischer Anforderungen, Umsetzung von Ausnahmen aufgrund von Kundenanforderungen Alle Schritte von Genehmigungsprozessen Updates, Patches und Änderungen der Netzwerkstruktur Konfigurationsänderungen	Antragsteller IT-Security-Organisation Administrator der Firewall
...		

In der oben abgebildeten Tabelle werden die wesentlichen Kriterien der Dokumentation an einem Beispiel aufgezeigt. Der Bezugspunkt, also der Unternehmenswert oder, wie hier, eine Gruppe an Unternehmenswerten, auf den



KAPITEL 15 – PRAXIS: AUFBAU EINES ISMS

sich die Dokumentation bezieht, dient dem Überblick. Ein Regelwerk definiert, was genau zu dokumentieren ist, und kümmert sich auch um die Frage, wer welches Dokument zu welchem Zeitpunkt einsehen, verändern oder löschen darf. Die Struktur der Dokumentation muss gewährleisten, dass jede Maßnahme, die aufgrund einer Anforderung oder im Rahmen der Risikobearbeitung implementiert wird, direkt auf die zugrunde liegenden Entscheidungsprozesse zurückgeführt werden kann. Die Dokumente verbinden damit den Output aller Arbeitsgebiete der IT-Security miteinander.

Das alles hört sich zunächst wie eine unüberschaubare und auch schwer umsetzbare Aufgabe an. Im Grunde handelt es sich aber nur um eine Strukturierung von meist bereits vorhandenen Aufzeichnungen.

15

Beantragt ein Benutzer, dass auf seinem Arbeitsplatzrechner ein bestimmter Patch nicht installiert wird, weil ansonsten seine Spezialanwendung nicht mehr funktioniert, so wird dies in den meisten Fällen in Form einer E-Mail geschehen. Statt diese E-Mail im E-Mail-Programm zu belassen, verschiebt sie der Manager IT-Security, der diese Art Fälle bearbeitet, in die ISMS-Dokumentation und verknüpft sie dort mit dem Unternehmenswert »Arbeitsplatzrechner von Herrn Mayer«. So wird diese Ausnahmeregelung später wiederzufinden sein. Der Mitarbeiter des Supports, der den Patch deinstalliert, fügt eine kurze Notiz zu diesem Vorgang hinzu, und schon ist der gesamte Prozess dokumentiert. Wird darüber in einer Besprechung diskutiert, dann sollte auch das Gesprächsprotokoll hinzugefügt werden (also zusätzlich alle Argumente und Beschlüsse, die den Vorgang beeinflusst haben).

Wichtig

Jedes Unternehmen muss für sich selbst entscheiden, welche Tiefe an Dokumentation es anstrebt und welche Anforderungen es damit erfüllen möchte. Sehr kleine Vorgänge zu dokumentieren, ist nur in denjenigen Fällen sinnvoll, in denen der Vorgang mit einem erhöhten Risiko einhergeht. Daraus folgt, dass auch, wenn es um die Dokumentation geht, die Höhe des Risikos bei der Auswahl der zu dokumentierenden Vorgänge eine große Rolle spielt.

Für den besseren Überblick folgt nun eine Auflistung möglicher Bestandteile einer ISMS-Dokumentation:



- Die Sicherheitsrichtlinie und alle Aufzeichnungen, die etwas über die von der Unternehmensleitung aufgestellten Ziele für die IT-Security-Organisation aussagen. Aus diesen Dokumenten, E-Mails, Gesprächsprotokollen und sonstigen Notizen werden die Art und der Umfang des IT-Security-Managements abgeleitet, und sie sind dementsprechend wichtig. Alle Mitarbeiter sollten die wesentlichen Dokumente kennen.
- Weitere Richtlinien wie die Klassifizierungsrichtlinie, die Richtlinie zum IT-Risikomanagement, Richtlinien für IT-Mitarbeiter, Verhaltensregeln für Mitarbeiter in Bezug auf Daten und den Umgang mit Gerätschaften des Unternehmens
- Regelungen bezüglich des ISMS selbst. Dazu gehören Richtlinien, was dokumentiert werden muss, wie dies zu geschehen hat und wer jeweils welche Art von Zugriff auf diese Dokumente erhalten soll. Hier können auch die Schnittstellen zu anderen Managementsystemen beschrieben werden. So ist es denkbar, dass das IT-Security-ISMS die Berichtswege des Qualitätsmanagementsystems nutzt oder unter Umständen sogar die gleiche Software.
- Alle Stufen des IT-Risikomanagements von der Analyse bis hin zur Definition von Maßnahmen und deren Überwachung. Diese Dokumente beinhalten regelmäßig den Auftraggeber, den Entscheider und die Instanz, die letztendlich eine Maßnahme umsetzt – jeweils mit Namen und Zeitpunkt. Insbesondere, wenn entschieden wird, dass ein erkanntes Risiko nicht behandelt wird, ist es interessant, den Entscheidungsprozess und die jeweiligen Entscheider zu kennen.
- Belange des Tagesgeschäfts eines Managers IT-Security. Dazu gehören auch unspektakuläre Vorgänge wie das Auftauchen eines Virus oder die Meldung über eine Häufung von Benutzerkonten, die aufgrund mehrerer Fehlversuche bei der Eingabe des Passworts geblockt wurden.
- Ergebnisse aus Audits
- Ereignisse, die vom Monitoring gemeldet werden
- Berichte aus IT-forensischen Untersuchungen

Die Lenkung von Dokumenten wurde bereits im Zusammenhang mit der Organisation von Richtlinien erwähnt, muss aber an dieser Stelle noch einmal erwähnt und verdeutlicht werden. Kein ISMS, schlichtweg kein Dokumentenmanagementsystem kann sinnvoll eingesetzt werden, ohne sich detailliert da-



KAPITEL 15 – PRAXIS: AUFBAU EINES ISMS

über Gedanken zu machen, wie die verwalteten Aufzeichnungen eingesetzt und in welchem Benutzerkreis sie veröffentlicht werden sollen. Auf der einen Seite muss gewährleistet sein, dass nur befugte Personen Einblick erhalten, und auf der anderen Seite gibt es Dokumente, die wiederum jeder Mitarbeiter kennen muss, und zwar immer in der letzten Version. Außer der Funktion Lesen sind diese Voraussetzungen auch für das Verändern und Löschen von Dokumenten umzusetzen.

Bezüglich der Dokumentenverwaltung innerhalb eines ISMS können folgende erforderliche Grundanforderungen an die Lenkung von Dokumenten definiert werden:

- Freigabeprozesse regeln, zumeist in Form von Workflows, wer welchen Vorgang genehmigen kann.
- Anhand der Versionierung von Dokumenten ist jederzeit erkennbar, welche Änderungen an einem Dokument vorgenommen wurden und wer diese zu welchem Zeitpunkt durchgeführt hat.
- Die Aktualität von Richtlinien, Anleitungen oder Notfallplänen sicherzustellen, ist eine Kernaufgabe. Dazu kommt die Erforderlichkeit, technisch zu garantieren, dass betroffene Mitarbeiter immer auch mit den jeweils aktuellen Dokumenten arbeiten. Das erfordert wiederum, dass Dokumente zentral abgelegt werden. Kopieren Mitarbeiter Dokumente auf weitere Datenträger, so ist nicht mehr zu garantieren, dass immer nur der Zugriff auf die jeweils aktuellste Version erfolgt.
- Regeln zur Verteilung bestimmen, wer welches Dokument zu welchem Zeitpunkt einsehen darf.
- Das Zugriffskonzept garantiert, dass jeweils nur befugte Personen Einblick in Dokumente erhalten. Dies gilt vor allem für Dokumente, von deren Inhalt Hinweise auf Schwachstellen abgeleitet werden könnten.
- Regelungen bezüglich der Lesbarkeit und Standardisierung haben wesentlichen Einfluss darauf, ob Dokumente auch gelesen und vor allem auch verstanden werden. Das betrifft Aufbau, Sprache und Schriftbild genauso wie die Organisation der Ablage.
- Auch Dokumente sind einer Klassifizierung unterworfen. In den meisten Fällen wird ein Zusammenhang zwischen dem Personenkreis der Empfänger und der Klassifizierung des Dokuments bestehen.



- Die Archivierung von Dokumenten, also die Speicherung in einer Form, in der keine Änderungen mehr möglich sind, stellt sicher, dass auch zu einem späteren Zeitpunkt unzweifelhaft Vorgänge nachvollzogen werden können.

Tipp

Es wird schnell erkennbar, dass je weitgehender Dokumente einem einheitlichen Aufbau folgen (vorzugsweise in einer definierten Sprache, auch in international tätigen Unternehmen), desto besser werden alle Instanzen damit umzugehen wissen.

Das bedeutet nicht, dass auf regionale Besonderheiten keine Rücksicht genommen werden muss – ganz im Gegenteil. Aber auch diese Ausnahmen sollten nur dann umgesetzt werden, wenn sie erforderlich werden. Das wird häufiger dann zutreffen, wenn es um Regelungen für Mitarbeiter geht, oder aber, wenn auf lokale gesetzliche Vorgaben eingegangen werden muss.

15

15.6 Softwaregestützter Aufbau eines ISMS

Die einzelnen Aufgabengebiete der IT-Security stehen nicht für sich alleine. Sie sind alle miteinander verbunden und haben zusätzlich noch zahllose Schnittstellen zu anderen betrieblichen Prozessen. So hat eine Entscheidung, die auf Basis einer Sicherheitsrisikoabwägung getroffen wird, oftmals direkte Auswirkungen auf die unternehmerischen Ziele wie z.B. das Erzielen von Profit. Andersherum ist es schlichtweg nicht möglich, in einem ISMS alle Auswirkungen zu berücksichtigen, denn dafür müssten alle Prozesse und deren Verflechtungen untereinander erfasst werden.

Ein softwaregestütztes ISMS wird also immer ein guter Kompromiss zwischen dem Aufwand, den man aufbringen muss, und dem Sicherheitsniveau, das man dadurch erreicht, sein müssen. Die Hoffnung, *das eine System* aufzubauen, das fortan die Geschicke des Unternehmens hinsichtlich der IT-Security steuert, wird in den allermeisten Fällen bereits bei der Budgetierung des Projekts begraben werden müssen. Zudem hat es sich in den letzten Jahren zunehmend gezeigt, dass ein ISMS einer bestimmten Größe unbeweglich und träge wird und der Aufwand zur Pflege dem Nutzen nicht mehr gerecht



wird. Das alles spricht nicht gegen den Aufbau eines ISMS, sondern vielmehr für ein mit Augenmaß geplantes Projekt, genau definierte Ziele und eine sinnvolle Auswahl der dazu erforderlichen Werkzeuge.

Wie in anderen Projekten auch muss man sich zunächst einmal im Unternehmen umsehen und die bereits im Einsatz befindlichen Tools erfassen. Nicht selten wird man dann auf Monitoring-Systeme, Programme zur Unterstützung von Audits, Dokumentenmanagementsysteme und Tools zur Unterstützung des Risikomanagements stoßen. Da die Form und der benötigte Leistungsumfang von Unternehmen zu Unternehmen stark variieren, existieren dementsprechend kleine bis große Lösungen. Das reicht dann von makrogestützten Excel- und Access-Lösungen bis hin zu datenbankbasierten Anwendungen. Ob diese einzelnen Anwendungen in das ISMS integriert werden sollen, hängt dann maßgeblich von Faktoren wie der Art der Datenhaltung, von Schnittstellen und generell der Nützlichkeit im Rahmen der Anforderungen ab.

15

15.6.1 Auswahl einer ISMS-Lösung

Die Kernaufgabe eines ISMS-Tools ist die Schaffung von Transparenz. Durch das Dokumentieren von Handlungen und die Unterstützung durch Workflows ist es möglich, Struktur in das Arbeitsgebiet der IT-Security-Organisation zu bringen. Dabei stehen die Unternehmenswerte, insbesondere Informationen in Form von Daten im Mittelpunkt. Alle möglichen Aktionen müssen sich also immer wieder auf die jeweils betrachteten Daten zurückführen lassen.

Die Risiken stehen dabei im Mittelpunkt der Betrachtung. Wird ein Risiko ermittelt und werden Maßnahmen zur Reduzierung implementiert, so beziehen sich diese immer auf einen bestimmten Unternehmenswert bzw. eine Kategorie an Unternehmenswerten. Eine Software auf einem Datenserver, die Schwachstellen aufweist, wird damit als Risiko abgebildet, das sich auf eben diesen Wert, den Datenserver, bezieht. Handelt es sich um eine Schwachstelle in einem Betriebssystem, so kann sich diese Schwachstelle auf eine ganze Reihe von betroffenen Servern beziehen.

Der Bezug ist deshalb wichtig, weil anhand des Risikos wiederum Maßnahmen definiert und Dokumentationen erzeugt werden. Soll der Erfolg der Umsetzung zu einem späteren Zeitpunkt untersucht werden, so muss man dafür den gesamten Entscheidungsvorgang nachzeichnen können.



SOFTWAREGESTÜTZTER AUFBAU EINES ISMS

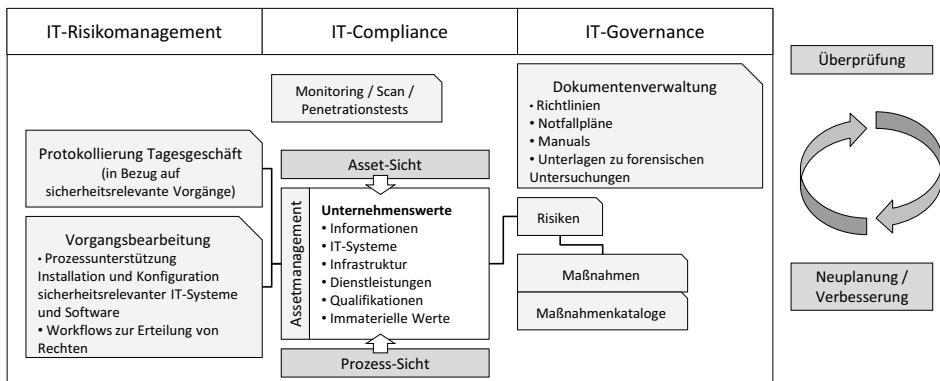


Abbildung 15.8: Grundlegende Bestandteile einer ISMS-Lösung

In Abbildung 15.8 ist dieser Zusammenhang abgebildet. Die Risiken und die daran angehängten Unternehmenswerte bilden den Mittelpunkt, um den sich die verschiedenen Funktionen des ISMS herum gruppieren.

Viele der auf dem Markt angebotenen Werkzeuge bieten eine Vielzahl weiterer Funktionalitäten, deren Darstellung an dieser Stelle nicht weiter verfolgt wird.

Der grundsätzliche Aufbau eines ISMS-Tools, also die Art der Verknüpfung verschiedener Objekte miteinander, ist das Hauptentscheidungskriterium bei der Auswahl. Neben diesem Punkt sind aber auch noch andere Kriterien wichtig, dazu gehören unter anderen:

- **Flexibilität:** Auch wenn ein Unternehmen ein ISMS gemäß einem Standard aufbaut, wird sich jedes ISMS immer im Detail von allen anderen unterscheiden. So kann ein Unternehmen mit drei Schutzstufen arbeiten oder mit fünf. Außerdem werden die Prozesse immer unterschiedlich ausgestaltet sein. Die Flexibilität, mit der ein Tool an eine bestehende Umgebung angepasst werden kann, bestimmt, inwieweit bestehende IT-Security-Prozesse übernommen werden können oder ob diese an ein Tool angepasst werden müssen. Im zweiten Fall bindet man sich an ein Tool und an unter Umständen für den Einsatzzweck nicht passende Rahmenbedingungen. Hier gilt der Grundsatz, dass sich ein ISMS-Tool immer an die Gegebenheiten des Unternehmens anpassen muss, und nicht andersherum.
- **Erweiterbarkeit:** Die Skalierbarkeit ist ein entscheidendes Kriterium für die Einsetzbarkeit eines Tools. Ein ISMS muss in der Lage sein, alle relevan-



vanten Vorgänge zu dokumentieren. Oftmals reicht es dafür nicht aus, nur den letzten Stand einer Richtlinie oder eines Protokolls abzulegen. Versionierung, Nachvollziehbarkeit und die Möglichkeit, Beziehungen zwischen Dokumenten und Werten herstellen zu können, benötigen eine ausgeklügelte Logik und setzen gewisse Techniken wie die Nutzung von Datenbanken voraus.

- **Mehrbenutzerfähigkeit:** Ein Benutzer beantragt den Zugriff auf einen externen FTP-Server, der Manager IT-Security gibt den Antrag frei, und der Administrator setzt die Regel um. Dieses einfache Beispiel zeigt, dass alleine in diesem Szenario bereits drei Rollen vertreten sind. Alle drei Schritte müssen aufgezeichnet werden, um später nachvollziehen zu können, wer etwas wollte, warum er dies wollte, wer etwas freigegeben hat und wer es umgesetzt hat. Nicht in jedem Unternehmen und in jedem Fall muss es sich dabei um drei unterschiedliche Personen handeln. Die Möglichkeit, technisch diesen Fall abbilden zu können, sollte aber offen gehalten werden.
- **Standardkonformität:** Ein ISMS ist etwas, das neben der Hebung des Sicherheitsniveaus auch schlicht dazu dient, Kunden zu zeigen: Bei uns sind eure Daten sicher. Oftmals dient es auch dazu, eine Zertifizierung zu unterstützen. Vielleicht geschieht dies nicht sofort, aber zumindest möchte man sich diese Möglichkeit nicht verstauen. Dazu kommt, dass der Beweis, »compliant« zu sein, einfacher fällt, wenn das eingesetzte ISMS den Kriterien von ISO 2700x und denen des BSI entspricht.
- **Workflows:** Sobald dokumentiert werden soll, wer eine bestimmte Entscheidung getroffen hat oder aber unterschiedliche Rollen wie »Benutzer«, »IT-Security« und »Administrator« im Spiel sind, wird sich die Frage stellen, ob sich Vorgänge nicht in Form von Workflows automatisieren lassen. In diesem Punkt unterscheiden sich die verschiedenen Tools erheblich. In einigen Produkten werden ganze Sicherheitsprozesse vorgezeichnet und durch sogenannte »Wizards« unterstützt. Da diesen vorgegebenen Abläufen einiges Know-how zugrunde liegt, sind diese Tools in der Regel im oberen Preissegment angesiedelt.

15.6.2 Darstellung der Risiken und der Unternehmenswerte

Die IT-Security verantwortet den Schutz vor Verlust von Vertraulichkeit, Verfügbarkeit und Integrität und eventuell weiterer Schutzziele. Das Ziel ist



damit im Grunde der Schutz des Know-hows des Unternehmens durch die Behandlung identifizierter Risiken. Da der Zugriff auf dieses Know-how auf vielfältigem Wege möglich ist, muss der Umfang des Schutzes auf alle diese Zugriffsmöglichkeiten erweitert werden. Aus diesem Grund ist z.B. nicht nur das Risiko für eine wichtige Kalkulationstabelle für ein neues Produkt zu betrachten, sondern gleichzeitig, und zwar mit derselben Aufmerksamkeit, auch für alle IT-Systeme, die den Zugriff auf diese Tabelle ermöglichen. Aus diesem Grund erweitert sich der Kreis der zu schützenden Unternehmenswerte – in diesem Beispiel um den Datenserver, das Netzwerk, über das die Tabelle übertragen wird, die Datensicherung und die Endgeräte, über die letztendlich der Zugriff erfolgt.

Grundsätzlich unterscheiden sich die Tools in ihrer Komplexität, und die hängt maßgeblich von der Art der Verwaltung von Risiken und Unternehmenswerten ab. So sind Tools auf dem Markt, die im Grunde ein Assetmanagement mit angehängtem Risikomanagement darstellen, oder aber Tools, die sich ganz auf das Risiko als zentralem Aufhänger konzentrieren.

Stellt man die Verwaltung der Werte in den Mittelpunkt, dann kann es schnell geschehen, dass die Anzahl der beteiligten Werte und deren Verbindungen untereinander sehr groß wird. Ein sinnvoller Aufbau des Assetmanagements, das Clustern von Systemen oder die Verknüpfung mit einem vorhandenen ist deshalb unabdingbar, um den Anforderungen nach Nachvollziehbarkeit, Aktualität und Übersichtlichkeit genügen zu können. In der Praxis ist es häufig anzutreffen, dass Werte in Gruppen zusammengefasst werden. Das bedeutet z.B. für die Gruppe der Arbeitsplatzrechner, dass nicht alle Rechner einzeln in die Übersicht des ISMS aufgenommen werden, sondern nur Platzhalter, die dann jeweils mehrere Maschinen repräsentieren.

Arbeitet man mit einem Tool, das die Risiken in den Vordergrund stellt, dann fehlt schnell der Bezug zu den Unternehmenswerten. Dadurch wird die Darstellung weniger komplex, erfordert aber das Fachwissen, jederzeit von Risiken auf Werte und von dort auf Maßnahmen schließen zu können. Das Definieren von Maßnahmen wird damit unpräziser und schwerer nachzuvollziehen. In einem solchen Tool genügt es, eine Reihe von Risikoabfragen z.B. pro Lokation oder Bereich des Unternehmens durchzuführen und das jeweilige Risiko einzuschätzen. Typische Fragen sind dabei:

- Entsprechen die Zutrittssysteme zum Campus den Vorgaben aus der Richtlinie zu Sicherheitszonen?



KAPITEL 15 – PRAXIS: AUFBAU EINES ISMS

- Werden die Bestimmungen zur Vergabe von Zugriffsrechten eingehalten?
- Sind die Server, die aus dem Internet erreichbar sind, gehärtet?

Die Herangehensweise ist in diesem Fall weniger detailliert, bringt aber den Vorteil mit sich, dass mittels eines Fragenkatalogs schnell eine Risikodarstellung möglich wird. Risikoreduzierende Maßnahmen werden direkt einem Risiko zugeordnet und verfolgt. Das Restrisiko, also das Risiko reduziert durch risikomindernde Maßnahmen, vermindert sich, nachdem eine Maßnahme kontrolliert abgearbeitet wurde.

15

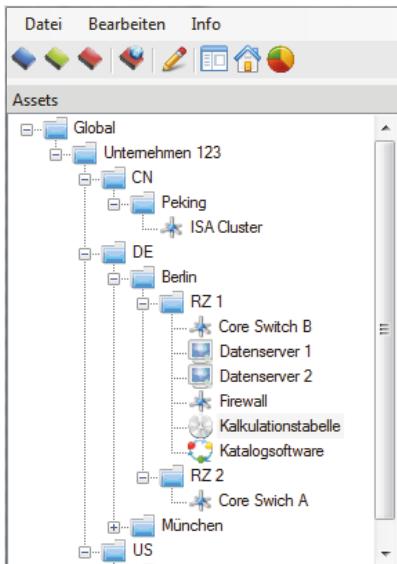


Abbildung 15.9: Beispiel: Verwaltung von Unternehmenswerten

Hinweis

Risiken und Unternehmenswerte sind die zentralen Elemente, mit denen in einem ISMS-Tool gearbeitet wird. Diese beiden Elemente müssen erfasst werden, um im weiteren Verlauf Restrisiken darstellen zu können und Maßnahmen mit realen Systemen in Verbindung zu bringen. Auch Richtlinien und Handlungsanweisungen wie Installationshandbücher und Wiederanlaufpläne können direkt mit einem Risiko oder einem Unternehmenswert wie z.B. einem Server verknüpft werden.



Die Gliederung von Risiken und Unternehmenswerten geschieht üblicherweise in einer Mischform zwischen geografischer und organisatorischer Sortierung. Auf diese Weise ist eine genaue örtliche Zuordnung möglich, und die Transparenz bleibt gewahrt, auch wenn die Anzahl der zu betrachtenden Risiken in die Hunderte geht.

15.6.3 Darstellung von Prozessen

Die Gliederung von Unternehmenswerten geschieht, wie im vorigen Abschnitt dargestellt, zunächst aufgrund der örtlichen und organisatorischen Platzierung im Unternehmen. Eine weitere Möglichkeit der Zuordnung ist die aufgrund der Zugehörigkeit zu einem Prozess. Je nach Aufgabenstellung ist auf diese Art und Weise gewährleistet, dass beide Perspektiven unterstützt werden. Außerdem wird es im Folgenden so auch möglich sein, Objekte wie Richtlinien nicht nur direkt an einem Wert, sondern auch an einem Prozess festzumachen.

15

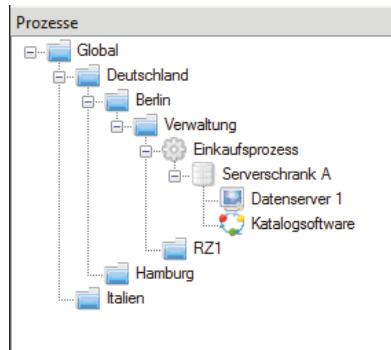


Abbildung 15.10: Darstellung eines Prozesses und zweier zugeordneter Unternehmenswerte

Prozesse zu betrachten, die direkt von IT-Systemen unterstützt werden, ist genauso wichtig wie Prozesse, die nur den Output anderer Prozesse als Input verwenden. So ist es sowohl erforderlich, alle IT-Systeme zu erfassen, die der Erstellung von Kalkulationen dienen (also Server, Anwendungen und Netzwerkkomponenten), als auch sekundäre Software wie z.B. das E-Mail-Programm, das zur Abstimmung genutzt wird. Alle Daten, die letztendlich zur Erstellung des finalen Kalkulationsblatts geführt haben, können später wichtig sein, z.B. wenn sie Gegenstand einer juristischen Auseinandersetzung werden.



Unternehmenswerte können, auch wenn sie wie z.B. ein Datenserver an sich nur einmal existieren, je nach Betrachtungsperspektive von unterschiedlicher Wichtigkeit für das Unternehmen sein. So kann der »Datenserver 1« im Zusammenhang mit dem Einkaufsprozess z.B. niedriger klassifiziert sein als im Zusammenhang mit den Protokollen von Vorstandssitzungen, die auch auf dem Server abgelegt sind. Damit können auch die Betrachtung aus Sicht des IT-Risikomanagements und davon abgeleitet die zu treffenden Maßnahmen zum Schutz der Daten unterschiedlich gestaltet sein. Es ist also durchaus sinnvoll, Prozesse abzubilden und zumindest teilweise daran auch die Risikobetrachtung aufzuhängen und Maßnahmen zu definieren.

15.6.4 IT-Risikomanagement

15

Risiko identifizieren und beurteilen

Die Identifizierung, die Beurteilung und die Behandlung von Risiken stehen im Mittelpunkt des IT-Security-Managements und damit auch im Mittelpunkt eines ISMS-Tools. Der erste Schritt ist demnach die Identifizierung von Risiken. Eine Vorgehensweise, dies zu erreichen, ist, über Fragenkataloge Risiken zu den Punkten aus Anhang A der ISO 27001 abzufragen. Eine weitere Möglichkeit ist es, aus der Perspektive der Unternehmenswerte mögliche Bedrohungen und Schwachstellen zu ermitteln und zu prüfen, ob diese ein Risiko darstellen. Ist dies geschehen, dann müssen die Risiken nach ihrer Kritikalität geordnet werden. Nicht jedes Risiko ist groß und muss sofort abgearbeitet werden.

In diesem Fall ergibt die Risikobetrachtung, siehe Abbildung 15.11, dass der Datenserver 1 als einer der Server nicht ausreichend bzw. nicht den Richtlinien entsprechend gehärtet wurde. Das heißt, dass nicht alle technischen Vorsehrungen getroffen wurden, um Betriebssystem und die installierte Software gegen Angriffe zu sichern. Dieses spezifische Risiko wird nach verschiedenen Kriterien bewertet, um möglichst genau feststellen zu können, wie ernst es genommen werden muss.

Die Wichtigkeit eines Risikos hat im Allgemeinen direkten Einfluss auf die Umsetzungsgeschwindigkeit von Maßnahmen, deren Auswahl und damit auch direkt auf die Kosten, die ein Unternehmen zu tragen bereit ist, um das Risiko zu minimieren oder vollständig zu vermeiden. Es handelt sich damit um einen verantwortungsvollen Vorgang, der direkt vom Eigentümer der



zugrunde liegenden Daten oder zumindest mit dessen Hilfe vorgenommen werden sollte.

The screenshot shows the 'RiskCard' application window. At the top, there's a logo of a red book and the title 'RiskCard'. Below the title, there are fields for 'Asset' (set to 'Datenserver 1'), 'Autor' (set to 'Harich'), and 'Letzte Änderung' (set to 'Änderungsdatum 09.11.2011 12:48'). On the left, there's a 'Template RiskCard' button. In the center, there are several sections: 'Name' (set to 'Server nicht gehärtet'), 'Art des Risikos' (a dropdown menu), 'Beschreibung' (text area containing 'Nicht zum Betrieb notwendige Netzwerkports sind geöffnet. Dahinterliegende Applikationen können angegriffen werden.'), 'Klassifizierung Risiko' (dropdowns for 'Eintrittswahrscheinlichkeit' (set to 'mittel'), 'Kosten im Eintrittsfall' (set to 'hoch (<50.000€)'), and 'Risikoklassifizierung' (set to 'Mittel')) , 'Risikobehandlung' (dropdown set to 'Minimieren'), 'Berechtigungen' (set to 'Verantwortlicher Harich' with a green checkmark icon), and 'Status' (checkbox 'Abgeschlossen' is unchecked). At the bottom right, there are buttons for 'Als Template speichern' (unchecked), 'Speichern', and 'Abbrechen'.

Abbildung 15.11: Zuordnung eines Risikos zum Unternehmenswert Datenserver 1

15

Risikobehandlung

Abhängig davon, wie die Behandlung eines Risikos aussehen soll, und abhängig von der Wichtigkeit des Risikos werden eine oder mehrere Maßnahmen definiert. Maßnahmen wiederum müssen umgesetzt werden, und damit sollte auch eine dafür verantwortliche Stelle definiert sein.

Maßnahmen können direkt aus dem Bauch heraus formuliert und festgelegt werden oder, und das ist empfehlenswert, sie entstammen einem im Vorfeld festgelegten Maßnahmenkatalog. Dies stellt sicher, dass Maßnahmen immer gleich lauten, wenn sie auch das Gleiche bewirken sollen. Der Maßnahmenkatalog wiederum sollte weitgehend unternehmensweit standardisiert sein. Noch besser ist es, wenn er auf einem Standard wie den BSI-Grundschutz-Katalogen oder auf Anhang A der ISO 27001 oder einem anderen anerkannten Maßnahmenkatalog basiert.

Ist dies der Fall, dann steigt die Vergleichbarkeit, und es ist eher sichergestellt, dass kompatibel zu den aktuell herrschenden Anforderungen gearbeitet wird.

519



KAPITEL 15 – PRAXIS: AUFBAU EINES ISMS

Der Verantwortliche für die IT-Compliance hat die Aufgabe, die Anforderungen zusammenzutragen, um daraus die Maßnahmenziele, also die übergeordneten Punkte, und daraus wiederum die einzelnen Maßnahmen abzuleiten.

The screenshot shows the 'ControlCard' application window. At the top left is a blue folder icon. Below it, the title 'ControlCard' is displayed above a button labeled 'ControlCard Template'. On the right side, there's a header row with columns for 'Asset' (containing 'Datenserver 1'), 'Autor' (containing 'Harich'), and 'Letzte Änderung' (containing '09.11.2011 12:58'). Below this, there are sections for 'Maßnahme' (with a dropdown menu set to 'gelb' and an unchecked checkbox for 'Abgeschlossen'), 'Workflow' (with 'Anforderer' set to 'ITSecurity' and 'Verantwortlich' set to 'Harich'), 'Umsetzung' (set to 'Administrators'), 'Katalog' (with a button 'Maßnahme auswählen' and a link 'Bezug zu Katalog'), and 'InfoCard' (a list box containing 'InfoCard' with a '+' and a delete icon). At the bottom right are buttons for 'Als Template speichern', 'Speichern', and 'Abbrechen'.

15

Abbildung 15.12: Zuordnung einer Maßnahme

15.6.5 Richtlinienmanagement

Die Erstellung von Richtlinien, Handlungsanweisungen und Handbüchern ist ein integraler Bestandteil des IT-Security-Managements. Diese Dokumente zu erstellen, ist eine Aufgabe in diesem Bereich, die Dokumente zu gruppieren und sie letztendlich angemessen zur Verfügung zu stellen, sind zwei weitere.

Dazu kommt die Anforderung aus Sicht der IT-Compliance, dass zu diesen eben erwähnten Arten von Dokumenten auch alle möglichen weiteren Informationen abzulegen sind. Dazu gehören Protokolle von Sitzungen, in denen über Details wie z.B. die Art der Risikobehandlung geredet und entschieden wurde, genauso wie Projektberichte und Ähnliches.

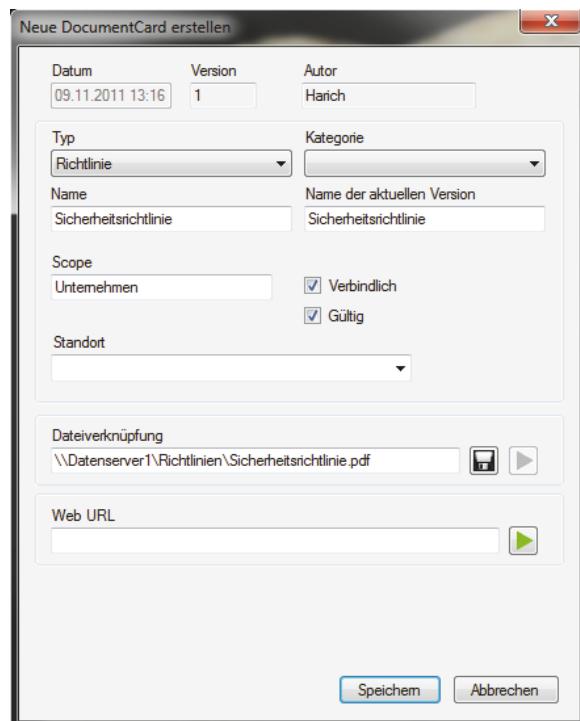


Abbildung 15.13: Verknüpfung mit einem Dokument

Alle diese Dokumente ergeben schnell eine unübersehbare Masse an Informationen, die kaum noch zu beherrschen ist. Das betrifft sowohl die Auffindbarkeit, die allgemeine Transparenz, aber auch – und das ist viel wichtiger – die Möglichkeit, diese adäquat regelmäßig zu aktualisieren. Aus diesem Grund sind zwei Anforderungen an eine integrierte Dokumentenverwaltung sehr wichtig: Die Dokumente sollten Werten oder Prozessen zuordenbar sein, um sie so zu strukturieren, und sie sollten versionierbar sein. Punkte wie Zugriffsregeln, Möglichkeiten zur Suche oder Details zur Ablage und Speicherung müssen zusätzlich betrachtet werden.

15.6.6 Arbeitsabläufe abbilden

Die meisten Daten, die ein ISMS ausmachen, kommen nicht aus dem Bereich der Richtlinien oder dem Richtlinienmanagement. Das größte Volumen entstammt der Dokumentation der täglichen Arbeit der IT-Security-Organisation. Jede Bewertung eines Risikos und damit verbunden die Maßnahmen, die



getroffen werden oder eben auch nicht, können zu einem späteren Zeitpunkt schwerwiegende Konsequenzen haben. Eine entgegen den Richtlinien, etwas tun zu dürfen, erteilte Freigabe oder Ausnahmen für die Unternehmensleitung kommen tagtäglich vor, obwohl sie zu einem erhöhten Risiko führen können.

Fordert der Geschäftsführer administrative Rechte auf seinem Laptop, obwohl dies per Richtlinie eigentlich verboten ist, so wird dies vermutlich dennoch umgesetzt werden. Wohl dem Manager IT-Security, der den gesamten Vorgang protokolliert, falls es zu einem späteren Zeitpunkt zu einem Datenverlust auf eben diesem Laptop kommt, ausgelöst durch einen Virus, der aufgrund der erweiterten Zugriffsrechte immensen Schaden anrichten konnte. Neben diesem drastischen Fall gibt es zahllose weitere kleine und große Entscheidungen, die getroffen werden müssen und dementsprechend auch dokumentiert werden sollten.

15

Kommentare an Werte geheftet, Risiken mit Beschreibungen oder auch Daten, die mit einem Vorgang verknüpft werden, bilden die Grundlage für die Abbildung des Tagesgeschäfts innerhalb des ISMS. Selbstverständlich ist in diesem Zusammenhang wichtig, dass Daten nicht nur abgelegt, sondern später auch wiedergefunden werden. Aus diesem Grund ist es notwendig, dass das ISMS-Programm auch hinsichtlich dieser Funktionalität einer durchgängigen Struktur folgt.

15.6.7 Berichte erstellen

Angenommen, die Datenbank ist gefüllt, alle wichtigen Risiken und Unternehmenswerte wurden erfasst, Prozesse definiert und Maßnahmen den Risiken zugeordnet, die nun von den Mitarbeitern abgearbeitet werden müssen. In diesem Stadium ist es von einiger Wichtigkeit, dass entsprechend der verschiedenen Sichten auf die Thematik Berichte erstellt werden können. Der Abteilungsleiter möchte sehen, welcher Mitarbeiter noch welche Maßnahmen zu erledigen hat, die Unternehmensleitung möchte wissen, welche kritischen Risiken verblieben sind, und der einzelne Mitarbeiter blickt täglich in seine eigene To-do-Liste und arbeitet sie ab.

Zu diesen häufig frequentierten Aussagen in Berichtsform kommen Auswertungen für Wirtschaftsprüfer und andere externe Auditoren hinzu.



15.7 Zertifizierung nach ISO 27001

Eine Zertifizierung anzustreben, heißt automatisch auch, die Regeln und Erfordernisse einer dritten Stelle anzuerkennen. Je anerkannter und international verbreiteter eine Zertifizierung ist, desto höher sind oft die Anforderungen, die an ein zertifizierungswilliges Unternehmen gestellt werden. Unterm Strich bedeutet dies, dass es im Normalfall handfeste Gründe geben muss, bevor Geld in die Hand genommen wird, um ein Stück Papier zu erarbeiten, auf dem steht, dass jemand einem ein Zertifikat verleiht.

Im Wesentlichen existieren zwei Triebfedern, die eine Zertifizierung im Bereich der IT-Security erstrebenswert machen:

- **Druck von außen:** Die Kunden, der Gesetzgeber oder die Wettbewerbssituation erfordern eine Zertifizierung. Dies ist vor allem dann der Fall, wenn Dritte sicherstellen wollen oder müssen, dass Daten in Ihrem Unternehmen sicher sind. Das kann z.B. dann der Fall sein, wenn ein Kunde seinem Lieferanten Daten überlässt, die der Lieferant benötigt, um ein Produkt zu entwickeln. Diese Daten verlassen in diesem Fall den Hoheitsbereich des Kunden, und um sicherzustellen, dass diese Daten nicht kompromittiert werden, verlangt der Kunde eine gewisse Sicherheit. Es wird davon ausgegangen, dass diese vorhanden ist, wenn er weiß, dass die IT-Prozesse beim Lieferanten auf Basis der ISO-27001-Methodik strukturiert sind und dies auch per Zertifikat nachgewiesen werden kann. Dies kann auch von der Branche abhängen: Werden sehr sensible Daten in einem Unternehmen, z.B. in einem Klinikum, verarbeitet, so werden sehr viel weitreichendere Anforderungen an IT-Systeme gestellt, als es in einem Unternehmen der Fall wäre, wo dies nicht geschieht. Gleich verhält es sich in Unternehmen, die unter das IT-Sicherheitsgesetz fallen, weil sie in dem Bereich der kritischen Infrastrukturen (KRITIS) zugeordnet werden. Aufgrund des Schutzbedarfs der Daten ist es sinnvoll, den Stand der IT-Security anhand einer Zertifizierung nachzuweisen. Ebenso ist dies bei Unternehmen denkbar, die mit der Bereitstellung und Speicherung von Daten ihr Geld verdienen. Nicht umsonst sind einige der ersten Zertifizierungen in Deutschland an Unternehmen verliehen worden, die sich mit dem Web-hosting beschäftigen.
- **Druck von innen:** Es sind viele Szenarien denkbar, in denen aus internen Beweggründen entschieden wird, eine Zertifizierung anzustreben. Häufig



KAPITEL 15 – PRAXIS: AUFBAU EINES ISMS

handelt es sich um sicherheitsrelevante Vorfälle, die einen nachhaltigen Eindruck auf die Unternehmensleitung machen und einen Denkprozess einleiten. Da es nicht immer wirksam ist, IT-Security Top-down zu verordnen, ist es umso sinnvoller, die Voraussetzungen einer international anerkannten Norm umzusetzen und in Form der Zertifizierung eine Art »Abnahme« anzustreben. Durch den nachhaltigen Verbesserungsansatz ist gleichzeitig gewährleistet, dass es sich nicht um eine Einmalaktion handelt. Die vielfältigen Meldeprozesse an das Management ermöglichen zudem eine garantierter Überwachung aller entscheidenden Vorgänge. Insbesondere Unternehmen, die erst damit beginnen, einen IT-Security-Bereich einzuführen, haben von vornherein die Möglichkeit, von den Best Practices der letzten 15 Jahre zu profitieren und ihre neue Organisationseinheit entsprechend der Norm aufzubauen.

15

Beide Punkte beinhalten Argumente, die IT-Security-Organisation auf Basis von ISO 27001 oder einem anderen Standard aufzubauen und zu betreiben. Dieses Ziel kann erreicht werden, indem als Abschluss und in den darauf folgenden Jahren wiederkehrend eine formelle Zertifizierung angestrebt wird, genauso gut aber auch ohne das formelle Papier. Um den Mehraufwand und die erzwungenen Rezertifizierungsläufe zu vermeiden, werden viele Firmen auf die Zertifizierung verzichten und zunächst mit dem Ziel einer allgemeinen Ausrichtung beginnen.

Da es nicht ausgeschlossen ist, dass nach einiger Zeit auch Anforderungen nach einem Zertifikat auftreten, ist es allerdings wichtig, von vornherein darauf zu achten, die Erfordernisse eines akkreditierten Prüfers zu kennen und die wichtigen Punkte zu beachten, um im Nachhinein den Zertifizierungsprozess zu beschleunigen.

Fällt die Entscheidung zugunsten einer Zertifizierung, dann führt an der ISO-27001-Norm kein Weg mehr vorbei. Das liegt vor allem an den nachfolgend aufgeführten Vorteilen:

- Die ISO 27001 ist eine international anerkannte Norm: Dies hat den großen Vorteil, dass vor allem international ausgerichtete Unternehmen einen deutlich leichteren Stand haben werden, eine Zertifizierung vorzubereiten. Dies gilt zum einen hinsichtlich interner Widerstände, die jedes umfangreiche Projekt mit sich bringt, als auch zum anderen für die Suche geeigneter Partner bei der Vorbereitung und Implementierung des ISMS.



- Durch die Ausrichtung der Norm ist es möglich, den Standard auf jedes Unternehmen jeglicher Größe und Geschäftsausrichtung anzuwenden.
- Die ISO 27001 ist nicht aus dem Nichts entstanden. Sie hat eine weit zurückreichende Geschichte hinter sich, die viele Entwicklungsschritte mit sich brachte. Ein wichtiger Aspekt ist dabei die sehr starke, inhaltliche Nähe zu den Normen ISO 9001 und ISO 14001. Diese Nähe macht es möglich, sehr ähnliche Managementprozesse zu etablieren und diese grundsätzlich auch gemeinsam abnehmen zu lassen. Diese Anlehnung war in der Vergangenheit auch durchaus erforderlich, um die Prozesse auf einen akzeptierten und praxisnah anzuwendenden Level zu bringen. Weitere Normen der 2700x-Reihe, die Teilespekte wie das Risikomanagement oder Anleitungen zum Gebrauch von Kennzahlen abdecken, sind bereits erhältlich. Dadurch werden Lücken geschlossen und Fragen beantwortet, die Manager IT-Security haben, wenn sie mit der Umsetzung von normierten Prozessen betraut werden.
- Die Normen ISO 27001 und ISO 27002 beschreiben mit klaren Aussagen, wann welche Anforderungen zu erfüllen sind, um ein PDCA-gesteuertes ISMS aufzubauen. Dadurch wird der Fortschritt bei der Implementierung sichtbar und messbar.
- Die oben aufgeführten Triebfedern für die Umsetzung eines standardisierten IT-Security-Betriebs werden durch die ISO 27001 bedient. Externen Vorgaben von Kunden kann die Norm genauso Genüge tun wie verschiedene gesetzliche Anforderungen.

Der Nutzen einer ISO-27001-Implementierung, zunächst unabhängig von der Erarbeitung eines Zertifikats, ist groß. Durch die Umsetzung eines kontinuierlichen Verbesserungsprozesses innerhalb der IT-Security wird diese auf ein professionelleres Niveau gehoben. Dies ist sicher auch mit anderen Ansätzen möglich, aber kein anderer bietet ein so großes Leistungsspektrum an Methoden und Best-Practice-Anleitungen.

15.7.1 Ansprechpartner

Ein Unternehmen, das eine Zertifizierung nach ISO 27001 anstrebt, wendet sich an eine akkreditierte Zertifizierungsstelle. Die Akkreditierungsstellen sorgen in Form einer Oberaufsicht dafür, dass die Zertifizierungsstelle gemäß den entsprechenden Normen agiert und ein definiertes Maß an Qualität



KAPITEL 15 – PRAXIS: AUFBAU EINES ISMS

einhält. Viele der Anforderungen werden in den Normen ISO 17021 und ISO 27006 definiert. Weitere Regeln werden durch Selbstverpflichtungen aufgestellt und ebenfalls durch die Akkreditierungsstelle überprüft.

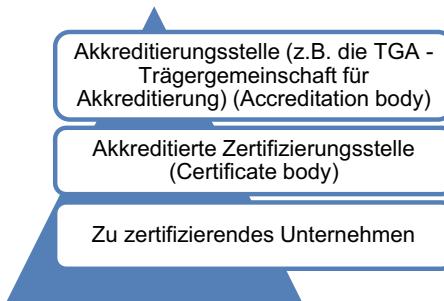


Abbildung 15.14: Zertifizierungsstellen

15

Die Akkreditierungsstellen überprüfen die Zertifizierungsstellen regelmäßig und legen dabei besonderes Augenmerk auf die Korrektheit der zugrunde liegenden Prozesse und den Ausbildungsstand der Mitarbeiter.

15.7.2 Prinzipien

Die Prinzipien, die für jede Zertifizierungsstelle gelten, werden in der ISO 17021 in Kapitel 4 aufgeschlüsselt. Es ist zu beachten, dass diese Regeln für die Auditierung jeglicher Arten von Managementsystemen ausgelegt sind.

Es handelt sich um die folgenden sechs als »vertrauensbildende Prinzipien« bezeichneten Grundsätze:

- Unparteilichkeit
- Kompetenz
- Verantwortlichkeit
- Offenheit
- Vertraulichkeit
- Offenheit gegenüber Beschwerden

Die Einhaltung dieser Grundsätze ist wichtig, um die Seriosität der Stellen zu gewährleisten. Vertrauen ist das wichtigste Gut für ein Unternehmen, das Audits durchführt. Der Verlust dieses Vertrauens schadet ihm und natürlich



auch dem Wert des letztendlich ausgestellten Zertifikats. Neben Maßnahmen wie eine Oberaufsicht über alle akkreditierten Zertifizierungsstellen, den oben aufgeführten Normen, die etliche Rahmenbedingungen formulieren, dienen die sechs Prinzipien als Basis für eine Reihe weiterer Regeln, die eingehalten werden müssen.

Wenn es um die Zertifizierung auf Basis einer Norm geht, stellt sich oft die Frage, inwieweit eine Zertifizierungsstelle auch beratend tätig werden darf. Obwohl es nur wenige akkreditierte Zertifizierungsstellen in Deutschland gibt, geht man häufig ganz automatisch davon aus, dass diese auch über den größten Erfahrungsschatz hinsichtlich der von ihnen auditierten Normen verfügen. Den Satz »Diejenigen, die mich beraten, werden wohl kaum später beim Zertifizierungs-Audit etwas auszusetzen haben« hört man häufig, und vollkommen falsch ist er vermutlich nicht. Deshalb ist es wichtig zu wissen, ab wann eine Zertifizierungsstelle in einem Umfang beratend tätig wird, die einer Zertifizierung durch dasselbe Unternehmen im Wege stehen würde.

Wichtig ist auch die Trennung von Zertifizierung und internem Audit. Ein internes Audit mit anschließenden Hinweisen auf Korrekturen in Abläufen und in den Einzelkomponenten des ISMS ist ein weitreichender Service. Wird dieser durch die Zertifizierungsstelle vorgenommen, so ist keine sinnvolle Trennung mehr von Beratung und Abnahme eines ISMS zu erwarten.

Es sind keine Interessenskonflikte zu befürchten, wenn es um die Kernaufgaben der Zertifizierungsstelle geht, also um die Festlegung von Terminen, der Überprüfung des ISMS und die Verfolgung der Abweichungen (*non-conformities*). Im Vorfeld allgemeine Schulungen anzubieten, ist ebenfalls erlaubt, genauso wie der Austausch von allgemein gehaltenen Informationen über die Inhalte des Zertifizierungsprozesses.

Die Akkreditierungsstelle überwacht die Kompetenz der Zertifizierungsstelle auf Basis der Vorgaben aus der allgemeingültigen Norm ISO 17021 und im Speziellen basierend auf den Vorgaben aus der ISO 27006. Dadurch soll sichergestellt werden, dass ein Audit-Team sowohl über das Detailwissen hinsichtlich der zu zertifizierenden Norm als auch hinsichtlich der Branche verfügt, in der das zu zertifizierende Unternehmen angesiedelt ist. Die Regeln für einen Auditor sind entsprechend diesen Anforderungen eng definiert. Um zu gewährleisten, dass ein Auditor sein Praxiswissen laufend ausbaut, ist er gezwungen, eine definierte Anzahl von Audits pro Jahr durchzuführen. Die



KAPITEL 15 – PRAXIS: AUFBAU EINES ISMS

Anforderungen an ein breites Wissen im Bereich der IT-Security und an das branchenspezifische Wissen sind ebenso hoch.

15

528



16 Awareness und Schulung

16.1 Kapitelzusammenfassung

Die Aufgabe des Managers IT-Security ist der Schutz von Informationen. Dafür wird ein IT-Security-Management aufgebaut und die entsprechenden Prozesse werden implementiert. Trotzdem wird er immer wieder feststellen, dass sicherheitskritische Ereignisse auftreten, obwohl für diese Fälle eigentlich vorgesorgt wurde. Spätestens an diesem Punkt wird er feststellen, dass es nicht ausreicht, über etwas Regeln zu legen, wenn die Mitarbeiter des Unternehmens diese nicht kennen, sie nicht zu nutzen wissen oder sich schlicht darüber hinwegsetzen. Eine Reaktion darauf ist die verschärzte Kontrolle mithilfe von Kennzahlen und der Überprüfung durch Monitoring-Systeme sowie die Ausweitung von Maßnahmen, das Bewusstsein der Mitarbeiter für die Wichtigkeit der Ziele der IT-Security zu stärken. Der letztere Punkt wird als Awareness-Steigerung bezeichnet und durch entsprechende Schulungsmaßnahmen unterstützt.

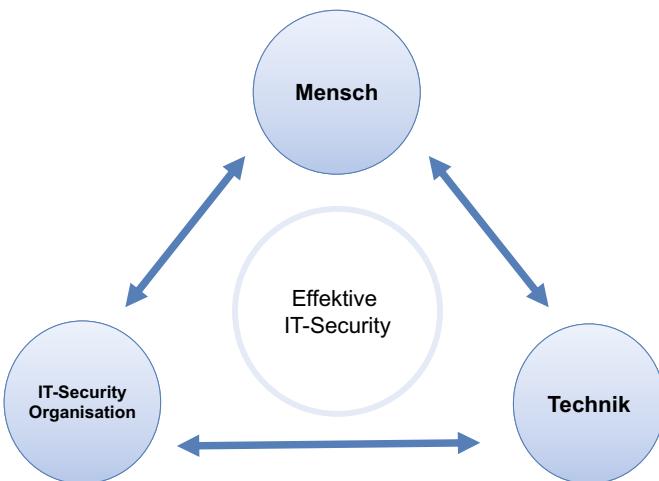


Abbildung 16.1: Drei Aspekte des IT-Security-Managements

Untersuchungen untermauern auf vielfältige Art die Sichtweise, dass Awareness-Maßnahmen eine große Rolle spielen. Ein Großteil aller Sicherheitsvor-



fälle geht auf das Konto interner Mitarbeiter oder sie sind zumindest darin verwickelt, und davon geschieht wiederum der größte Teil unabsichtlich, also ohne kriminellen Hintergrund. Dieser Anteil kann durch die Initiierung von Awareness-Maßnahmen signifikant verringert werden. Das Nutzen-Kosten-Verhältnis ist zudem im Allgemeinen günstiger, als es bei zusätzlichen technischen Maßnahmen der Fall wäre. Trotzdem muss immer bedacht werden, dass nur ein Mix von Maßnahmen, die alle Perspektiven abbilden, zu einem akzeptablen Ergebnis führen wird (siehe Abbildung 16.1).

16.2 Verbesserungsprozess

16

Einmalig angesetzte Schulungen oder einmalig verteilte Flyer haben nachweislich keinen nachhaltigen Effekt. Wichtiger ist, neben der Aufgabe, die richtige Mischung von Maßnahmen zu finden, auch deren wiederholte Anwendung: Nachhaltigkeit durch ständige Wiederholung. Das Ziel dieses Prozesses ist das Erreichen einer Sicherheitskultur auf einem Level, der im Einklang mit den Zielen der IT-Security-Organisationen steht und der die technischen Maßnahmen ideal unterstützt.

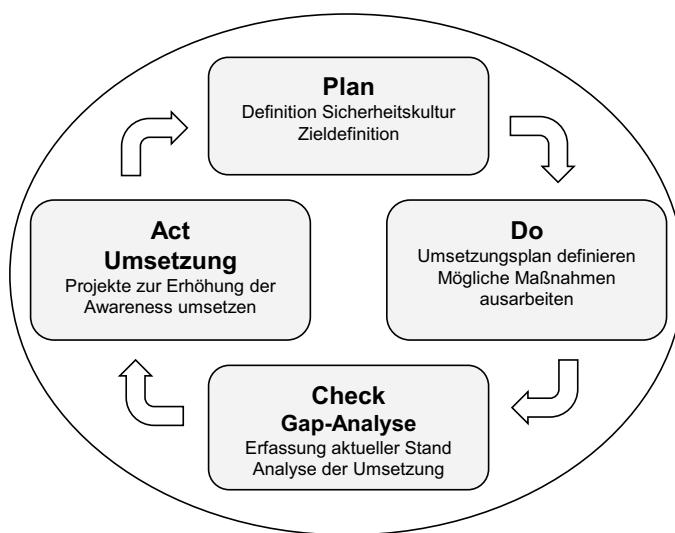


Abbildung 16.2: Regelkreislauf Verbesserung Awareness

Zentraler Punkt ist das Security Awareness Management (SAM). Es dient der Analyse und zielgerichteten Weiterentwicklung des Sicherheitsbewusstseins



in Bezug auf Unternehmensdaten. Innerhalb des Regelkreises, wie er in Abbildung 16.2 abgebildet ist, umfasst er die Funktionen der Planung, der Durchführung und der Kontrolle von Awareness-Maßnahmen.

Zu Beginn steht auch hier die Aufgabe, die Ausgangssituation zu analysieren. Zu bewerten ist der Stand, auf dem die Sicherheitskultur im Unternehmen aktuell steht. Daraus werden die erforderlichen Maßnahmen abgeleitet, um die übergeordneten Ziele zu erreichen, die dann in Form von Awareness-Projekten implementiert werden. So macht es wenig Sinn, in einem Unternehmen, in dem Datensicherheit bislang kein Thema war, ohne weitere Erläuterungen die Mitarbeiter dazu aufzufordern, alle selbst erstellten Daten zu klassifizieren und so in den IT-Risikomanagementprozess einzubringen.

Solange das grundlegende Verständnis und auch die persönliche Einsicht fehlen, dass diese Schritte wirklich erforderlich sind, wird ein so komplexes Vorgehen nicht flächendeckend gelingen. Es muss ein persönliches Verlangen eines jeden Data Owners sein, sich nicht nur um die Qualität der Informationen, sondern auch um deren Sicherheit zu sorgen. Der Prozess, sich diese Aufgabe zu eigen zu machen, ist das erklärte Ziel von Awareness-Maßnahmen. Wie diese technisch umgesetzt werden können, wird dann in entsprechenden Schulungen aufgezeigt.

16.3 Voraussetzungen für eine Sicherheitskultur

Technische Lösungen unterstützen Arbeiten, die ein Mensch zuvor geplant hat. Ungeplante Ereignisse oder Ereignisse von einer unvorhergesehenen Komplexität können nur vom Menschen auch adäquat gelöst werden. Aus diesem Grund ist das aktive und bewusste Zusammenspiel der Mitarbeiter und der technischen IT-Security-Prozesse von elementarer Wichtigkeit. Die Technik arbeitet deterministisch, während der Mensch in der Lage ist, kreativ und flexibel zu agieren. Um alle Mitarbeiter zu befähigen, korrekt zu handeln, müssen die folgenden grundlegenden Voraussetzungen geschaffen werden:

- Die Leitungsebenen müssen in die Pflicht genommen werden, IT-Security-Prozesse aktiv einzufordern und vorzuleben. Es muss Teil der Unternehmenskultur werden.
- Alle Mitarbeiter müssen um ihre Verantwortung und den daraus erwachsenden Verantwortlichkeiten wissen.



KAPITEL 16 – AWARENESS UND SCHULUNG

- Eine Sensibilisierung der Mitarbeiter für die wesentlichen möglichen Problemstellungen, bei denen ihre Mithilfe vonnöten ist, muss vorgenommen werden.
- Vorgaben und Empfehlungen sowie die zugrunde liegenden Prozesse müssen schriftlich festgehalten werden und die entsprechenden Schriftstücke jedem zur Verfügung stehen.
- Alle Mitarbeiter müssen durch Schulungen auf einen Kenntnisstand gebracht werden, der sie befähigt, Situationen richtig einzuschätzen und daraus die richtigen Handlungen abzuleiten.

Das Ziel der Anstrengungen lässt sich folgendermaßen zusammenfassen: Die Sicherheitskultur muss fester Bestandteil der Unternehmenskultur werden. Nur eine vollständige Durchdringung aller Bereiche ermöglicht Sicherheit auf einem hohen Niveau.

16

Tipp

Die Sicht auf die Informationssicherheit ist eng verknüpft mit dem kulturellen Umfeld und dem Land, in dem ein Mitarbeiter aufgewachsen ist. Aus diesem Grund muss bei der Entwicklung von Projekten, die das Ziel haben, die Awareness anzuheben, auch darauf gesteigert Rücksicht genommen werden. Dies betrifft zum einen die Priorisierung von Maßnahmen als auch die Ausgestaltung der Mittel wie Poster oder Flyer und geht so weit, dass für einzelne Länder gegebenenfalls eigene Farbmuster oder Logos entwickelt werden.

Jeder Mitarbeiter macht sich außerhalb des Unternehmens ständig Gedanken über Sicherheitsthemen. Wie notiere ich am besten die PIN für die EC-Karte, damit sie auch wirklich sicher ist? Wie kann ich den Einbruchsschutz für meine Wohnung verbessern? Vertraue ich meinem Nachbarn meinen Wohnungsschlüssel an, wenn ich im Urlaub bin? Alle diese Fragen hat sich jeder schon einmal gestellt, und es ist die Aufgabe der Sicherheitskultur, diese Fragen und mögliche Antworten auf die Belange des Unternehmens zu projizieren. Damit verringert sich der Abstand zwischen den persönlichen, individuellen Zielen und den Zielen des Unternehmens maßgeblich und erleichtert die Umsetzung von Maßnahmen.



16.4 Erfassung der Sicherheitskultur

Da Kultur nicht in dem Maße gemessen werden kann wie IT-Systeme, müssen an dieser Stelle zusätzliche Werkzeuge eingesetzt werden. Zwei Arten von Kennzahlen können hierbei hilfreich sein:

1. **Selbstauskunft:** Das eigene Empfinden der Mitarbeiter, wie sie mit Situationen umgehen, in denen sicherheitsrelevante Entscheidungen getroffen werden müssen.
2. **Statistische Kennzahlen:** Messung der Entwicklung von Vorkommnissen, die auf Missachtung bestehender Regelungen zurückgeführt werden können.

Das wichtigste Instrument im Rahmen der Awareness-Bildung ist das Interview von Mitarbeitern. Durch Fragebögen, die regelmäßig durch relevante Personengruppen ausgefüllt und im Anschluss daran ausgewertet werden, kann die subjektive Stimmung erfasst werden. Üblicherweise erfolgt die Erfassung der Daten über das Intranet und fließt im Anschluss, anonymisiert, in eine zentrale Datenbank. Die Bandbreite an unterschiedlichen Fragestellungen ist groß, und so kommen vor allem die folgenden Abfragethematiken vor:

- Wie geht der Mitarbeiter mit einer bestimmten Situation um?
- Wie beurteilt ein Mitarbeiter den Nutzen einer bestimmten Regelung für sich und für das Unternehmen?
- Hält ein Mitarbeiter die Mehrarbeit, die durch Einsatz einer Maßnahme wie z.B. der Verschlüsselung von Anhängen an E-Mails entsteht, für angemessen?
- Welche Vorschläge hat ein Mitarbeiter, das Sicherheitsniveau zu erhöhen?

Alle Facetten der IT-Security-Organisation können, abhängig von der Zusammensetzung der Interviewgruppe, abgefragt werden. Dadurch ist es möglich, festzustellen, in welchen Teilbereichen der IT-Security-Strategie eventuell Schwachstellen bestehen bzw. von außen gesehen werden. Wichtige Kernbereiche der IT-Security, die abgefragt werden sollten, sind:

- **IT-Security-Organisation:** Sind Ansprechpartner für die Mitarbeiter vorhanden?



- **Sicherheitsziele:** Sind die Mitarbeiter mit den Zielen der IT-Security-Organisation vertraut und können sie den Bogen zu den Unternehmenszielen schlagen?
- **Kommunikation:** Sind alle für die Mitarbeiter relevanten Regelungen bekannt und verständlich erklärt worden? Wissen die Mitarbeiter um ihre Pflichten im Rahmen der bestehenden Regelungen und wie sie welche Methoden diesbezüglich anwenden müssen?
- **Sicht auf die Leitungsebene:** Werden die Ziele der IT-Security von den Vorgesetzten gelebt? Ist erkennbar, dass die Ziele der IT-Security Teil der Unternehmensziele sind?
- **Problemlösungen:** Werden Probleme der Mitarbeiter schnell und kompetent gelöst? Stehen technische Lösungen für alle in den Regelungen geforderten Maßnahmen zur Verfügung und können die lokalen Sicherheitsverantwortlichen damit umgehen?
- **Personalabteilung:** Werden neue Mitarbeiter vor der Einstellung damit vertraut gemacht, welche Verantwortung sie bezüglich der Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität tragen? Werden Änderungen in der Anstellung, z.B. der Abteilungswechsel, so kommuniziert, dass die entsprechenden Zugriffsrechte angepasst werden? Werden bei Beendigung des Arbeitsverhältnisses alle erforderlichen Maßnahmen getroffen, um den weiteren Zugriff auf Unternehmensdaten auszuschließen?
- **Technische Umsetzung:** Entsprechen die technischen Hilfsmittel wie ein Verschlüsselungstool den Anforderungen der Mitarbeiter in Bezug auf Funktionalität und Handling? Ist die Integration von Sicherheitstools in die tägliche Arbeit sinnvoll umgesetzt?

16.5 Top-down-Ansatz

Die Einstellung der Leitungsebenen und das Maß, in dem sie die Sicherheitsziele vorleben, bestimmt in großem Maße auch das Verhalten der Mitarbeiter. Deshalb ist es sinnvoll, bei der Umsetzung von Awareness-Maßnahmen bei diesen Ebenen zu beginnen und sich dann nach unten vorzuarbeiten. Es ist kein Geheimnis, dass die Umsetzung von Regelungen zur Sicherstellung von Informationssicherheit für den einzelnen Mitarbeiter Mehrarbeit bedeutet. Je höher also die Auslastung ist und je höher damit der individuelle Druck steigt, desto näher liegt es, sich durch Ignorieren von Vorgaben Luft zu verschaffen.



Dem kann durch technische Maßnahmen vorgebeugt werden, z.B. indem kritische Prozesse durch den Einsatz von Workflows in einer Art und Weise gesteuert werden, dass der vorgegebene Pfad nicht verlassen werden kann. Diese Vorgehensweise ist aber nur in Einzelfällen bis ins Detail durchzuhalten und damit führt kein Weg daran vorbei, nicht nur die Ergebnisse der Arbeit von Mitarbeitern zu bewerten, sondern auch die Zielerreichung unter dem Gesichtspunkt der IT-Security.

Der Lernprozess ist langwierig und mühsam und ein Lockerlassen kann schnell dazu führen, dass die guten Vorsätze wieder über Bord geworfen werden. IT-Security ist in dieser Hinsicht kein Selbstläufer, auch wenn nachgewiesen ist, dass, je höher die Sicherheitskultur in einem Unternehmen ist, das Fehlerpotenzial sinkt, was die Anwendung von Maßnahmen betrifft, und auch die Toleranz sinkt, erkannte Sicherheitsverstöße zu ignorieren und hinzunehmen.

16

16.6 Awareness-Projekte

Nach der Ableitung von erforderlichen Maßnahmen zur Steigerung der Awareness aus dem Delta zwischen dem aktuellen Status der Sicherheitskultur und den Zielen und Erwartungen, die sich das Unternehmen stellt, folgt im nächsten Schritt die Umsetzung von Awareness-Projekten. Die Zielsetzung ist die Erreichung des in der Plan-Phase definierten Soll-Zustands. Abhängig vom aktuellen Stand der Sicherheitskultur können die Maßnahmen eher korrigierender Art sein oder aber grundsätzlich darauf abzielen, ein neues Niveau zu erreichen. Abhängig von der Zielrichtung werden selbstverständlich auch die einzelnen Aktionen ausgerichtet werden müssen.

Ein Großteil der Zeit und Mühe, die für die Durchsetzung von Sicherheitsanforderungen aufgebracht wird, konzentriert sich in den meisten Unternehmen darauf, Vorgaben zu entwickeln und diese punktgenau umzusetzen. Dazu gehört z.B. eine Passwortrichtlinie, die statt nicht komplexer Passwörter nach neuer Richtlinie komplexe Passwörter vorschreibt. Die technische Umsetzung erfolgt durch Konfiguration der entsprechenden Identity-Management-Systeme und die organisatorische Umsetzung kann durch eine E-Mail an alle Benutzer stattfinden. In einem Unternehmen, das über eine funktionierende und allgemein anerkannte und gelebte Sicherheitskultur verfügt, werden die Mitarbeiter die neue Regelung aufnehmen, deren Wichtigkeit ver-



stehen und es als Teil ihrer Verantwortung sehen, diese auch umzusetzen. In einem Unternehmen mit nicht voll ausgeprägter Sicherheitskultur werden die Mitarbeiter vermutlich die Vorgabe lesen, verstehen und notgedrungen auch umsetzen. Durch die Mehrarbeit wird aber auch Unmut oder Unverständnis entstehen, was wiederum dazu führt, dass vermehrt Zettel mit dem neuen komplexen Passwort unter Tastaturen und an Monitoren zu finden sind. In diesem Fall hat der Aspekt Mensch versagt und gefährdet damit die Zielerreichung.

Das Beispiel zeigt, dass Awareness-Maßnahmen, die rein auf Vorgaben basieren, nicht unbedingt allein zum Ziel führen. Aus diesem Grund findet seit einigen Jahren ein Wechsel bzw. eine Erweiterung um Verständnis- und Sensibilisierungsmaßnahmen statt. Die Maßnahmen, die an das Verständnis der Mitarbeiter appellieren, nennt man auch soziokulturelle Maßnahmen. Eine typische Vorgehensweise ist in diesem Fall der Vergleich zwischen alltäglichen Sicherheitsmaßnahmen im privaten Bereich und den Erfordernissen im Unternehmen. Dazu kann z.B. der Vergleich zwischen dem Abschließen des Wohnhauses zum Schutz der darin befindlichen Wertgegenstände und dem Sichern der Unternehmensinformationen herangezogen werden. Das Ziel ist es dabei, ein Verständnis dafür zu erzeugen, dass sowohl die privaten Eigentümer Schutz benötigen und dass das Gleiche auch für das Know-how des Unternehmens Gültigkeit hat. Versteht und akzeptiert dies ein Mitarbeiter, dann wird er auch versuchen, die Sorgfalt in beiden Fällen auf einem ähnlichen Niveau zu halten.

Typische Maßnahmen zur Steigerung der Awareness sind:

- Handlungsanweisungen
- Zusätze zum Arbeitsvertrag
- Poster und Flyer
- Werbegeschenke, um die IT-Security-Organisation im Unternehmen bekannt zu machen und deren Existenz und damit auch deren Zuständigkeit ins Bewusstsein zu rücken
- Weiterbildungsmaßnahmen, die den Hintergrund hinter einer Richtlinie erklären und die Wichtigkeit, z.B. anhand einer Risikodarstellung, erläutern
- Berichte in Unternehmenszeitschriften und im Intranet



- Lernprogramme, vor allem im Bereich des Datenschutzes, da hier eine Sensibilisierung auch gesetzliche Grundlagen hat
- Sensibilisierungsvideos, entweder selbst entworfen und produziert oder eingekauft

Ein Großteil der Maßnahmen hat das Ziel, dass jeder Mitarbeiter in seine Handlungen, in seine alltäglichen Aufgaben und Projekte auch den Aspekt der Informationssicherheit einbezieht.

Awareness-Projekte zielen darauf hin, die Gewohnheiten von Personen zu verändern. Veränderungen werden wiederum individuell völlig unterschiedlich gerne oder ungerne gesehen. Es geht dabei um einen Eingriff in das Gewohnte und Sichere und damit in die Bedürfnisse der Mitarbeiter. Natürlich gilt dies nicht für jede geringfügige Maßnahme, aber schon Vorgaben, wie zum Beispiel, dass auch IT-Mitarbeiter nur noch in Begleitung des Rechenzentrum betreten dürfen, greift in eine Reihe von Arbeitsvorgängen ein und kann negative Reaktionen hervorrufen. Vertrauen mir meine Vorgesetzten nicht mehr? Wie soll ich dann noch meine Arbeit schaffen? Dies sind typische Fragen, die im Rahmen der Erläuterungen zum Projekt unbedingt adressiert werden müssen. Es ist leicht zu erkennen, dass die Umsetzung von Awareness-Maßnahmen Einfühlungsvermögen erfordert und zu einem nicht unwesentlichen Teil aus Psychologie besteht.





Index

A

Access Control List 164
Access-Point 309
Account 176
Act-Phase 482, 506
Ad-hoc-Modus 308
AES 262
Aktiengesetz 75, 193
Aktiv-Aktiv-Cluster 242
Aktiv-Passiv-Cluster 242
Alarmierung 67
Alarmierungskette 213
Analyse
 forensische 431
Angriffsart 419
 Diebstahl von Kennwörtern 423
 Social Engineering 420
 Verwertung von Müll 422
 Zugriffsrecht 420
Angriffspfad 328, 418
Angriffsvektor 163, 415, 418
Annualized Loss Expectancy 460
Anstellung
 Phasen 178
Asset siehe Unternehmenswert
Assetmanagement 319, 351, 367
Audit 128, 133, 387, 391
 Abschlussbericht 408
 Durchführung 404
 Fragnenkatalog 405–406
 Themenkatalog 405
 Vorbereitungen 403
 Vor-Ort-Audits 397
Aufgabenspektrum
 Manager IT-Security 38
Auftragsverarbeitung 285
Auftragsverarbeitungs-Vertrag 286
Ausfallsicherheit 240
Ausfallzeit 236

Authentisierung 164
 what you are 165
 what you have 164
 what you know 164
Authentizität 335
Autorisierung 164
Availability management siehe Verfügbarkeitsmanagement
Awareness 154, 529

B

Background-Check 256
Backup siehe Datensicherung
Balanced Scorecard 463
Bauliche Maßnahme 242, 246, 329
Bedrohung 317, 321, 328
 Listen 353
 vorsätzliche 330
 zufällige 330
Behavioral Analysis 380
Belastbarkeit 171, 235
Bell-LaPaluda-Modell 167
Benutzeraccount siehe Account
Bereitschaftsregelung 217
Betriebshandbuch 173
Betriebsübergabe 173
Beweismittelkette 429
Beweissicherung 429
Bewertungsmatrix 143
Biba-Modell 168
Big Data 380
Brandschutz 214
Bring your own device 150
Browser
 Risikofaktor 301
BS 7799 80
BSI 78, 253
BSI-Grundschutz 89, 367



INDEX

- BSI-Standard 100-1 87
 BSI-Standard 100-2 88
 BSI-Standard 100-3 88
 BSI-Standard 100-4 89
 Bundesamt für Sicherheit in der Informati-
 onstechnik siehe BSI
 Bundesdatenschutzgesetz 95, 159, 250, 252
 Bürgerliches Gesetzbuch 100
 Business Continuity Management siehe IT
 Business Continuity Management
 Business-Impact-Analyse 48, 185, 194, 200,
 205, 212, 238, 384
 Checkliste 228
- C**
- CEO Fraud 29, 421
 Chain of custody 429, 436
 Chance
 Risiko 371
 Checkliste
 Business-Impact-Analyse 228
 Cloud Computing 280
 Notfallorganisation 229
 Notfallpläne 230
 Rechenzentrum 230
 Wiederanlaufpläne 230
 Check-Phase 482, 505
 Chiffrierung 269
 Cloud 272
 Anforderungskatalog des BSI 279
 Bring Your Own Key 281
 Community Cloud 275
 Datenschutz 285
 Hybrid Cloud 275
 Infrastructure-as-a-Service 278
 NIST 272
 On-demand self service 272
 Platform-as-a-Service 277
 Private Cloud 274
 Public Cloud 274
 Software-as-a-Service 277
 Storage-as-a-Service 277, 279
 Verschlüsselung 280
 Zugriffsgeschwindigkeit 273
 Cloud Computing
 Checkliste 280
- Cloud Computing C5 89
 Cluster 233, 242
 COBIT 76
 Common Criteria 94
 Computer Security Incident Response Team
 424
 Computerkriminalität 415
 CSIRT 380, 424
 Cybercrime-Versicherung 216, 372
- D**
- DAC-Modell 166
 Data Owner 35, 141, 166
 Daten
 vs. Informationen 22
 Datendiebstahl
 durch Außenstehende 418
 durch eigene Mitarbeiter 416
 Passwort 423
 Dateneigentümer 35
 Daten-Informationseigentümer 35
 Datenintegrität 267
 Datenschutz 65, 95, 144, 285
 Datenschutzbeauftragter 65
 Datensicherung 241
 Datensparsamkeit 37
 Datenträgerkontrolle 262
 Datenübertragung 262
 Delphi-Methode 355, 358
 Denial of Service 300
 Digitale Signatur 271, 304
 Digitalisierung 158
 Disaster Recovery 223
 Discretionary Access Control 166
 DMZ 250
 Do-Phase 482, 503
 Dynamische Redundanz 241
- E**
- Ein-Faktor-Authentisierung 166
 Eingabekontrolle 265
 Eintrittswahrscheinlichkeit 357, 367
 Elektronische Signatur 304
 E-Mail 179, 298
 Risikofaktor 299
 Verschlüsselung 300



Entschlüsselung 269
Ereignisbaumanalyse 358
Erpressersoftware 29
EU-Datenschutz-Grundverordnung 74, 95, 158, 275
EU-DSGVO siehe EU-Datenschutz-Grundverordnung
Excessive privilege 161, 420

F

Facility-Management 68
False positive 385
Fehlzustandsbaumanalyse 358
Fingerabdruck 165
Firewall 290, 418, 424
 Applikations-Firewall 293
 Next-Generation-Firewall 294
 Paketfilter-Router 293
 Personal Firewall 290
 Proxyserver 290, 293
 Regelwerk 295
 Stateful Inspection 293
Forensik siehe IT-Forensik
Forensische Analyse 431
 Anforderungen 435
 Methoden 436
Forensische Untersuchung 434, 437
Funktionelle Redundanz 243
Funktionstrennung 36

G

Gap-Analyse 493
Gebäudemanagement 68
Gefährdung 317, 328
Geheimtext 269
Geltungsbereich 348
 ISMS 486
Genehmigungsprozess 181
Geschäftsprozesse
 Priorisierung 198
 Übersicht 195
Gesetz gegen den unlauteren Wettbewerb 100
Gewaltenteilung 59, 62
Gewalttrennung 160

GmbH-Gesetz 75, 158
Governance 43
Governance Risk und Compliance Software 161
Grundschutz 86
Grundschutz-Kataloge des BSI 374

H

Haftung 158
Handelsgesetzbuch 193
Hochverfügbarkeit 236
Honeypot 308, 432
Honeytoken 432
HTTP 294, 298

I

ICMP 227
Identifikation 164
Identitätsmanagement 176
Identity management siehe Identitätsmanagement
Incident-Management 413
Incident-Response-Prozess 429
Industrie 4.0 213
Information 22
 Schutzbedarf 23
 vs. Daten 22
Informationssicherheitspolitik 136
Infrastrukturmodus 309
Initiator 322, 330, 419
Integrität 334
Interne Revision 68
Internet 298
Intrusion-Detection-System (IDS) 306, 439
Intrusion-Prevention-System 307
ISMS 81, 136, 459, 473
 Geltungsbereich 486
 softwaregestütztes 511
ISMS-Handbuch 137, 144
ISO 14000 507
ISO 15504 93, 144, 448, 495
ISO 17021 526
ISO 27000
 Zertifizierung 82



INDEX

- ISO 27001 79, 81, 90, 96, 366, 374, 445, 458, 474
Kennzahlen 453
- ISO 27002 81, 83, 374
- ISO 27004 446, 452
- ISO 27005 79, 141, 317, 487
- ISO 27006 79, 526
- ISO 27018 279
- ISO 27035 413
- ISO 31000 93, 317
- ISO 31010 93, 358
- ISO 9000 507
- ISO 9001 482
- IT Business Continuity Management 153, 186, 204
- IT-Administrator 69
- IT-Compliance 41, 71
- IT-Forensik 413, 436
- IT-Grundschutz-Kataloge 85
- ITIL 76, 92, 446
- IT-Infrastruktur 502
- IT-Risikomanagement siehe Risikomanagement
- IT-Security-Strategie 30
- IT-Sicherheitsgesetz 25, 52, 523
- IT-Sicherheitsrichtlinie 148
- K**
- Kapazitätsmanagement 234
- Katastrophe 191, 211
- Kennzahlen 48, 134, 360, 443
gute 451
schlechte 452
Vergleichbarkeit 452
- Kernprozesse 199
- Klartext 269
- Klassifizierung 142, 333, 337
- Klassifizierungsrichtlinie 140, 142, 167, 336, 488
- Konfigurationsmanagement 234
- Kontinuitätsmanagement siehe Verfügbarkeitsmanagement
- Kontinuitätsstrategie 207
- Korrelation von Sicherheitseignissen 380
- Krise 191, 210
- Krisenstab 217, 219
- Kritische Prozesse 199
- Kryptografie 269
- Kryptosystem 269
- Kumulationsprinzip 337
- L**
- Lagebild 379
- Laptopverschlüsselung 265
- Least privileges 161
- Leitlinie 128
- Level of Assurance 258
- Live-Forensik 431
- M**
- MAC-Modell 167
- Mail-Spoofing 299
- Malware siehe Schadsoftware
- Manager IT-Security
Aufgabenspektrum 38
Rolle 50
- Mandatory Access Control 166
- Masquerading 421
- Maßnahme 330, 367, 374
bauliche 242, 246, 329
soziokulturelle 536
technisch-organisatorische 252
- Maximum Tolerable Downtime (MTD) 238
- Maximumprinzip 337
- Metrics siehe Kennzahlen
- Monitoring 227, 377
Agent 385
Betrachtungsebenen 380
LogFile-Monitoring 228, 265, 385
Protokoll-Monitoring 385
System-Monitoring 382
- N**
- Need-to-know-Prinzip 36, 178, 259
- Nichtabstreitbarkeit 335
- Nine-Steps-Model 465
- NIST 800-10 293
- Notfall 191, 210
- Notfallbewältigung 217, 221, 428



Notfallhandbuch 208, 211, 219
Notfallkonzept 207
Notfallkrisenstab 219
Notfallmanagement 89, 186, 192, 203, 428
 Checklisten 228
 Richtlinien 205
Notfallorganisation 217
 Checkliste 229
Notfallplan 174
 Checkliste 230
Notfallstrategie 206
Notfallübung 225
Notfallvorsorge 211
Notfallwiederherstellung 223

O

Obfuscation 176
Offline-Forensik 431
Online-Forensik 431
Operative Sicherheit 249
Operatives Risiko 322
Organigramm
 Organisation 49, 58
Organisation
 Organigramm 49, 58
OSI-Modell 294
OWASP 174

P

Passwort 164
 Datendiebstahl 423
Patchmanagement 241
PDCA-Regelkreis 80, 183, 477, 482
Penetrationstest 171, 302, 398
Personalmanagement 150
PGP 300
Phishing 28
Ping 382
Plan-Phase 482, 488
Poka Yoke 37
Port-Scan 303
Post-mortem-Analyse 431
Potenzieller Schaden 359
Predictive Maintenance 213
Pre-shared Key 270, 310

Prinzipien 35
Privacy by default 37
Privacy by design 37
Produktionsnetze 291
Proxyserver 297
Prozessdefinition 194
Prozesse
 kritische 199
Prozesserfassung 194
Pseudonymisierung 275
Public-Key-Verfahren 270

Q

Qualitätshandbuch 171
Quantitative Risikoermittlung 319

R

RAID 233, 242
Ransomware 29
RBAC-Modell 168
Rechenzentrum
 Checkliste 230
Redundante Systeme 186, 234, 241, 243
Redundanz
 dynamische 241
 funktionelle 243
 statische 241
 strukturelle 242
Redundanzeffekt 338
Reifegradmodell 344
Restrisiko 320, 360, 428
Return on Security Investment (ROSI) 446
Revision 392
 interne 68
Richtlinien 127, 129, 520
 Attribute 130
 Basisrichtlinien 135
 Geltungsbereich 139, 149
 IT-Sicherheitsrichtlinie 148
 IT-Systemrichtlinie 152
 Kategorisierung 130
 Klassifizierungsrichtlinie 140, 167, 336, 338, 488
Notfallmanagement 205
Richtlinien-Pyramide 129



INDEX

- Risikomanagement 146, 487
Sicherheitsrichtlinie 136, 487
Überarbeitungsintervall 148, 152
Verfügbarkeitsmanagement 234
Versionierung 133
- Risiko 315, 322
 akzeptieren 370
 Chance 371
 operatives 322
 reduzieren 371
 verlagern 372
 vermeiden 372
- Risikoanalyse 86, 318
- Risikoarten 316, 366
- Risikobehandlung 318, 365, 368, 487
- Risikoberechnung 360, 362
- Risikobewertung 318, 356, 368
- Risikoeigentümer 35
- Risikoerfassung 319
- Risikoermittlung
 quantitative 319
- Risikofaktor
 Browser 301
 E-Mail 299
- Risikoidentifizierung 318
- Risikokatalog 366
- Risikomanagement 44, 311
 Richtlinien 146
- Risikomanagementkultur 314
- Risikomanagementprozess 320
- Risikomatrix 364
- Risikowert 364
- Risk Owner 35
- Risk owner 35
- Role-Based Access Control 166
- Rollen 50
 Datenschutzbeauftragter 63, 65
 Gebäudemanagement 68
 Interne Revision 68
 IT-Administrator 69
 IT-Risikomanager 57
 IT-Security Professional 57
 IT-Security-Auditor 57
 IT-Security-Organisation 57
 lokale IT-Security-Manager 64
 Manager IT-Compliance 57
 Manager IT-Security 50, 57
- RBAC-Modell 168
Sicherheitsingenieur 68
Unternehmensleitung 56
Werkschutz 67
- S**
- S/MIME 300
Sabotage 329
SANS 326
Sarbanes-Oxley Act 25, 76, 136
Schaden 316
 potenzieller 359
- Schadensanalyse 197
- Schadensklasse 143, 344
- Schadsoftware 28, 299
- Schlechte Kennzahlen 452
- Schulung 154, 529
- Schulungsmaßnahmen 215
- Schutzbedarf 34, 142, 336, 338
 Informationen 23
- Schutzbedarfsfeststellung 333
- Schutzstufe 142, 336
- Schutzziele 33, 142, 324, 333
 abhängige 333
 alleinstehende 333
- Schwachstelle 319, 321, 325, 329, 418
 logische 326
 physische 328
- Schweregrad 209
- Scope siehe Geltungsbereich
- Scorecard 226
- Security Awareness Management 530
- Security Information and Event Management siehe SIEM
- Security Operation Center siehe SOC
- Security-Management 24
 Aufgaben 44
- Security-Strategie 30
- Selbstauskunft 399
- Self-Assessment siehe Selbstauskunft
- Separation of duties siehe Gewalttrennung
- Service Delivery Assurance 234
- Service Level Agreement 216, 235, 381
- Service-Level-Management 234



Sicherheit
operative 249
Sicherheitseinstufung 167
Sicherheitsergebnis 380, 413
Sicherheitsingenieur 68
Sicherheitsklasse 167
Sicherheitslandschaft 395
Sicherheitsleitbild 145
Sicherheitsrichtlinie 136, 148, 487
Sicherheitsstrategie 30
Sicherheitsvorfall 306
SIEM 379, 386, 398, 424, 444
Signator 304
Signatur
digitale 271, 304
elektronische 304
Signaturgesetz 304
Single Loss Expectancy 461
Smartcard 164
SMTP 299
SOC 379, 424
Social Engineering 420
Software 169
Application Service Provider 170
Betriebshandbuch 173
Eigenentwicklung 170, 174
im Auftrag entwickelt 170
Implementierung 172
Kaufsoftware 170
Qualität 170, 175
Versionierung 176
Softwaregestütztes ISMS 511
Softwarequalität 170
Sorgfaltspflicht 158, 193
Spam-Mail 300
SPICE 344, 448
Standardisierung 36, 158, 182
Statische Redundanz 241
Steuerungsfunktion 47
Störung 191, 209
Strafgesetzbuch 100
Strategie der IT-Security 30
Strategieübersicht 467
Strukturelle Redundanz 242
Syslog 386
Systeme
redundante 186, 234, 241, 243

T
Technisch-Organisatorische Maßnahmen
252
Telefonliste 211
Telekommunikationsgesetz 76, 99
Telemediengesetz 99
TISAX 101
TKG 76
Token 164
TOM siehe Technisch-Organisatorische
Maßnahme
TPISR 102
Transparenz 158
Transport Layer Security 300
Transportkontrolle 261
Two signatures 161

U
Übertragungskontrolle 261
Unternehmensleitung
Rollen 56
Unternehmenssicherheit 66
Unternehmensstrategie 312
Unternehmenswert 142, 199, 514
Untersuchung
forensische 434, 437
Urheberrechtsgesetz 100
USB 261

V
VDA-ISA-Katalog 407
Verband der Automobilindustrie 134
Verfassungsschutz 27
Verfügbarkeit 183, 186, 235, 266, 334
Verfügbarkeitsklasse 237
Verfügbarkeitskontrolle 266
Verfügbarkeitsmanagement 192, 233
Richtlinien 234
Verhaltensanalyse 417
Verhaltenserkennung siehe Behavioral
Analysis
Verhältnismäßigkeitsprinzip 299, 332
Verschlüsselung 160, 268, 327
asymmetrisch 270
Cloud 280



INDEX

E-Mail 300
öffentlicher Schlüssel 271
privater Schlüssel 271
Public-Key-Verfahren 271
Schlüssel 270
Schlüsselaustausch 270
symmetrisch 270
Verteilungseffekt 338
Vertraulichkeit 334
Vieraugenprinzip 36, 151, 160
Virenschutz siehe Schadsoftware
Vor-Ort-Audit 397
VPN 263, 270

W

Wahrscheinlichkeitsvorhersagen 357
WannaCry 353, 425
WEP 310
Werkschutz 67
Wiederanlaufplan
 Checkliste 230
Wiederherstellbarkeit 266
Wiederherstellung 241

Wireless LAN 308
Wirtschaftlichkeit 36
Wirtschaftsspionage 27
WLAN 308
Workflow 181, 514
WPA 310

Z

Zero Day Attack 326
Zertifizierung
 Grundschutz 88, 91
 ISO 27001 82, 91, 351, 523
Zertifizierungsstelle 525
Zivilprozessordnung 304
Zugangskontrolle 254, 256
Zugriffskontrolle 151, 166, 259
Zugriffskontrollmodell 166
Zugriffsrecht
 Angriffsart 420
Zutrittskontrolle 67, 215, 254
Zuverlässigkeit 266
Zwei-Faktor-Authentifizierung 164