



Thomas W.  
Harich

3. Auflage



# **IT-Sicherheitsmanagement** **Das umfassende Praxis-Handbuch**

für IT-Security und technischen Datenschutz nach ISO 27001

- **Aufgaben des IT-Security-Managers**
- **Informationssicherheit ausarbeiten**
- **IT-Sicherheitskonzepte einrichten**
- **Information Security Management System aufbauen**

# Inhaltsverzeichnis

	<b>Einleitung</b>	15
<b>1</b>	<b>Umfang und Aufgabe des IT-Security-Managements</b>	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
<b>2</b>	<b>Organisation der IT-Security</b>	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

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
<b>3</b>	<b>IT-Compliance</b>	<b>71</b>
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	Fragenkatalog	109
<b>4</b>	<b>Organisation von Richtlinien</b>	<b>127</b>
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

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
<b>5</b>	<b>Betrieb der IT-Security</b>	<b>155</b>
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
<b>6</b>	<b>IT Business Continuity Management</b>	<b>185</b>
6.1	Kapitelzusammenfassung	185
6.2	Einführung	186
6.3	Abgrenzung der Begriffe	190

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
<b>7</b>	<b>IT-Notfallmanagement</b>	<b>203</b>
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

<b>8</b>	<b>Verfügbarkeitsmanagement</b>	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
<b>9</b>	<b>Technische IT-Security</b>	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

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
<b>10</b>	<b>IT-Risikomanagement</b>	<b>311</b>
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

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
<b>11</b>	<b>Sicherheitsmonitoring</b>	<b>377</b>
11.1	Kapitelzusammenfassung	377
11.2	Einführung	378
11.3	Ebenen des Monitorings	380

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
<b>12</b>	<b>IT-Security-Audit</b>	<b>391</b>
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
<b>13</b>	<b>Management von Sicherheitsereignissen und IT-Forensik</b>	<b>413</b>
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

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
<b>14</b>	<b>Kennzahlen</b>	<b>443</b>
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
<b>15</b>	<b>Praxis: Aufbau eines ISMS</b>	<b>473</b>
15.1	Kapitelzusammenfassung	473
15.2	Einführung	474
15.3	ISMS in Kürze	474

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
<b>16</b>	<b>Awareness und Schulung</b>	<b>529</b>
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
	<b>Index</b>	<b>539</b>

# 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 Informationssicherheit 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

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.

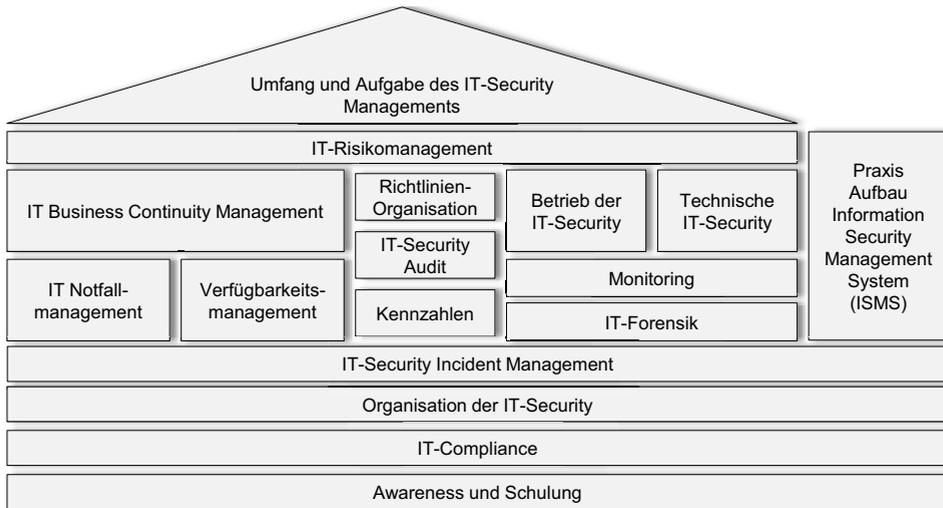
Andere, und damit sind wir wieder bei den vielen Wegen angekommen, die zum Ziel führen, sind Neueinsteiger oder Quereinsteiger. Vielleicht kommen sie aus der IT-Abteilung und haben zuvor Server administriert oder Softwareprojekte geleitet. In manchen Fällen waren sie davor aber auch im Controlling oder 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

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 vergegenwärtigen, 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

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 entgegensetzt. 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

### 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 Virensch scanner, 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

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-Leitung 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.

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-

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:

- **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

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-

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, publikumswirksame 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 einigen 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

## 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

# 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  
    Fragenkatalog 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 Verfügbar-  
    keitsmanagement  
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

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 Informationstechnik 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-Grund-  
 verordnung  
 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  
 Gewaltentrennung 160

GmbH-Gesetz 75, 158  
 Governance 43  
 Governance Risk und Compliance Software  
   161  
 Grundschatz 86  
 Grundschatz-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 Identitätsma-  
 nagement  
 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 2700  
   Zertifizierung 82

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  
 Korrelierung von Sicherheitsereignissen 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  
 Prozessfassung 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

- 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 Gewaltentrennung
  - Service Delivery Assurance 234
  - Service Level Agreement 216, 235, 381
  - Service-Level-Management 234

- Sicherheit  
 operative 249  
 Sicherheitseinstufung 167  
 Sicherheitsereignis 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

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  
   Grundschatz 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