

# 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>