

# Inhaltsverzeichnis

<b>Einleitung</b>	<b>15</b>
<b>I Umfang und Aufgabe des IT-Security Managements</b>	<b>19</b>
<b>I.1 Kapitelzusammenfassung</b>	<b>19</b>
<b>I.2 Einführung</b>	<b>19</b>
<b>I.3 Informationen und Daten</b>	<b>20</b>
<b>I.4 IT-Security Management ist wichtig</b>	<b>22</b>
<b>I.5 Wie gefährdet sind die Unternehmensdaten</b>	<b>24</b>
<b>I.5.1 Sicht des Verfassungsschutzes</b>	<b>24</b>
<b>I.5.2 Öffentliche Wahrnehmung</b>	<b>25</b>
<b>I.5.3 Die eigene Wahrnehmung</b>	<b>27</b>
<b>I.6 Begrifflichkeiten</b>	<b>28</b>
<b>I.7 Selbstverständnis der IT-Security-Organisation</b>	<b>29</b>
<b>I.8 Grundregeln</b>	<b>32</b>
<b>I.9 Umfang des IT-Security Managements</b>	<b>34</b>
<b>I.9.1 Pfeiler der IT-Security</b>	<b>36</b>
<b>I.9.2 Aufgaben des IT-Security Managements</b>	<b>40</b>
<b>I.10 IT-Security zwischen Nutzen und Kosten</b>	<b>43</b>
<b>2 Organisation der IT-Security</b>	<b>47</b>
<b>2.1 Kapitelzusammenfassung</b>	<b>47</b>
<b>2.2 Einführung</b>	<b>47</b>
<b>2.3 Rollen innerhalb des IT-Security Managements</b>	<b>48</b>
<b>2.3.1 Manager IT-Security</b>	<b>49</b>
<b>2.3.2 Unternehmensleitung</b>	<b>53</b>
<b>2.3.3 Weitere Rollen</b>	<b>53</b>

2.4	Verankerung im Unternehmen	54
2.4.1	IT-Security und der Datenschutz	56
2.4.2	Zusammenspiel mit anderen Sicherheitsbereichen	57
2.4.3	IT-Security im Organigramm	60
<b>3</b>	<b>IT-Compliance</b>	<b>67</b>
3.1	Kapitelzusammenfassung	67
3.2	Einführung	68
3.3	Standards	72
3.3.1	ISO 2700x-Reihe	73
3.3.2	Standards des Bundesamts für Sicherheit in der Informationstechnik	79
3.3.3	Gegenüberstellung ISO 2700x und BSI-Grundschutz	83
3.3.4	ITIL	86
3.3.5	Weitere Standards	87
3.4	Gesetze	88
3.4.1	Bundesdatenschutzgesetz	88
3.4.2	Weitere Gesetze	92
<b>4</b>	<b>Organisation von Richtlinien</b>	<b>95</b>
4.1	Kapitelzusammenfassung	95
4.2	Einführung	96
4.3	Strukturierung von Richtlinien	97
4.4	Beschreibung und Kategorisierung	98
4.5	Pflege und Lenkung von Richtlinien	99
4.6	Richtlinien und Audits	101
4.7	Verschiedene Richtlinien	102
4.7.1	Sicherheitsrichtlinie	103
4.7.2	Klassifizierungsrichtlinie	108
4.7.3	Richtlinie zum IT-Risikomanagement	111
4.7.4	IT-Sicherheitsrichtlinie	112

4.7.5	IT-Systemrichtlinien	116
4.8	Von der Theorie in die Praxis	118
<b>5</b>	<b>Betrieb der IT-Security</b>	<b>121</b>
5.1	Kapitelzusammenfassung	121
5.2	Einführung	121
5.3	IT-Security und der IT-Betrieb	123
5.4	Betriebliche Grundsätze	124
5.4.1	Ableitung aus gesetzlichen Vorschriften	124
5.4.2	Vertragswesen	125
5.4.3	Administrative Tätigkeiten	125
5.4.4	Trennung von Funktionen	126
5.4.5	Prinzip der geringsten Rechte	127
5.5	IT-Security-Prozesse	127
5.5.1	Zugriffs- und Zugangskontrolle	128
5.5.2	Sicherheit von Kaufsoftware	134
5.5.3	Sichere Softwareentwicklung	138
5.5.4	Identitätsmanagement	141
5.5.5	Genehmigungsprozesse	145
5.5.6	Standardisierung	146
5.5.7	Unterstützung des IT-Betriebs	147
<b>6</b>	<b>IT Business Continuity Management</b>	<b>149</b>
6.1	Kapitelzusammenfassung	149
6.2	Einführung	150
6.3	Notfallmanagement und Verfügbarkeitsmanagement	153
6.4	Gesetzliche Rahmenbedingungen des Business Continuity Managements	154
6.5	Business Impact-Analyse	154
6.5.1	Erfassung und Priorisierung der Geschäftsprozesse	155
6.5.2	Business Impact-Analyse in der Praxis	160

6.6	Weitere Einflussfaktoren	161
7	<b>IT-Notfallmanagement</b>	163
7.1	Kapitelzusammenfassung	163
7.2	Einführung	163
7.3	IT-Notfallmanagement	164
7.4	Richtlinie zum Notfallmanagement	165
7.5	Ableitung von Notfallstrategien	166
7.6	IT-Notfallkonzepte erstellen	167
7.6.1	Schweregrade	169
7.6.2	Notfallvorsorge	170
7.7	Notfallorganisation	175
7.7.1	Organisationsstruktur	175
7.7.2	Kompetenzen und Zuständigkeiten	176
7.7.3	Notfallhandbuch	177
7.8	Notfallbewältigung	180
7.9	Notfallübungen	183
7.10	Überprüfung des IT-Notfallmanagements	184
7.11	Monitoring im Rahmen des IT Business Continuity Managements	185
7.12	Checklisten Notfallmanagement	186
7.12.1	Checkliste Business Impact-Analyse	187
7.12.2	Checkliste Notfallorganisation	188
7.12.3	Checkliste Notfallpläne und Wiederanlaufpläne	188
7.12.4	Checkliste Rechenzentrum	189
8	<b>Verfügbarkeitsmanagement</b>	191
8.1	Kapitelzusammenfassung	191
8.2	Einführung	191
8.3	Richtlinie zum Verfügbarkeitsmanagement	192

<b>8.4</b>	<b>Verfügbarkeit</b>	<b>193</b>
<b>8.4.1</b>	Klassifizierung von Verfügbarkeit	194
<b>8.4.2</b>	Vorgehensweise	195
<b>8.4.3</b>	Berechnung der Verfügbarkeit	196
<b>8.5</b>	Ausfallsicherheit	197
<b>8.6</b>	Ausprägungen von Redundanz	198
<b>8.6.1</b>	Strukturelle Redundanz	199
<b>8.6.2</b>	Funktionelle Redundanz oder unterstützende Redundanz	200
<b>8.6.3</b>	Informationsredundanz	200
<b>8.7</b>	Redundante Hard- und Software	201
<b>8.8</b>	Virtualisierung	202
<b>8.9</b>	Bauliche Maßnahmen zur Steigerung der Verfügbarkeit	203
<b>9</b>	<b>Technische IT-Security</b>	<b>205</b>
<b>9.1</b>	Kapitelzusammenfassung	205
<b>9.2</b>	Einführung	206
<b>9.3</b>	Technisch-organisatorische Perspektiven	208
<b>9.3.1</b>	Zutrittskontrolle	209
<b>9.3.2</b>	Zugangskontrolle	211
<b>9.3.3</b>	Zugriffskontrolle	213
<b>9.3.4</b>	Weitergabekontrolle	215
<b>9.3.5</b>	Eingabekontrolle	218
<b>9.3.6</b>	Auftragskontrolle	219
<b>9.3.7</b>	Verfügbarkeitskontrolle	221
<b>9.4</b>	Verschlüsselung	222
<b>9.4.1</b>	Begriffsbestimmungen	222
<b>9.4.2</b>	Symmetrische Verschlüsselungssysteme	223
<b>9.4.3</b>	Asymmetrische Verschlüsselungsverfahren	224
<b>9.5</b>	Cloud Computing	225
<b>9.5.1</b>	Definition von Cloud Computing	227
<b>9.5.2</b>	Dienstleistungen in der Cloud	228

9.5.3	Risikofaktoren	229
9.5.4	Datenschutzrechtliche Aspekte	234
9.5.5	Vertragliche Vereinbarungen	236
9.6	Betrieb von Firewalls	237
9.6.1	Paketfilter und Application-Gateways	239
9.6.2	Firewall-Regelwerk	241
9.6.3	Proxyserver	242
9.7	Internetzugang und Nutzung von E-Mail	243
9.7.1	Risikofaktor E-Mail	244
9.7.2	Verschlüsselung von E-Mails	245
9.7.3	Risikofaktor Internetbrowser	245
9.8	Penetrationstests	246
9.9	Digitale Signatur	248
9.10	Intrusion-Detection-Systeme	250
9.11	Wireless LAN	252
10	<b>IT-Risikomanagement</b>	255
10.1	Kapitelzusammenfassung	255
10.2	Einführung	256
10.3	IT-Risikomanagement im Unternehmenskontext	256
10.4	Akzeptanz des IT-Risikomanagements	258
10.5	Operatives IT-Risikomanagement	259
10.5.1	Vorgehensweise	261
10.5.2	IT-Risikomanagementprozess	264
10.5.3	Übergeordnete Risikobetrachtung	265
10.5.4	Schwachstellen	268
10.5.5	Bedrohungen	271
10.5.6	Zusammenspiel von Bedrohungen, Schwachstellen und Maßnahmen	273
10.5.7	Verhältnismäßigkeit	274

10.6	Schutzbedarfsfeststellung	275
10.6.1	Schutzziele	276
10.6.2	Schutzstufen	278
10.6.3	Prinzipien	279
10.6.4	Feststellung des Schutzbedarfs	280
10.6.5	Veränderung des Schutzbedarfs	285
10.6.6	Widersprüchliche Schutzziele	286
10.6.7	Schadensklassen	287
10.6.8	Abbildung des Datenflusses	287
10.6.9	Entscheidungsfindung auf Basis des Schutzbedarfs	288
10.7	Risikoanalyse	290
10.7.1	Kritische Unternehmenswerte erfassen	290
10.7.2	Risikoermittlung	294
10.7.3	Risikobewertung	297
10.8	Quantitative Darstellung von Risiken	300
10.8.1	Grundlagen der Risikoberechnung	301
10.8.2	Risikoberechnung im Beispiel	303
10.8.3	Risikomatrix	305
10.8.4	Risikokatalog	307
10.9	Risikobehandlung	308
10.9.1	Risiko beurteilen	309
10.9.2	Risiko akzeptieren	311
10.9.3	Risiko reduzieren	312
10.9.4	Risiko vermeiden	313
10.9.5	Risiko auf Dritte verlagern	313
10.10	Maßnahmen definieren	314
10.10.1	Maßnahmentypen	314
10.10.2	Individuelle Maßnahmenkataloge	316
II	<b>Monitoring</b>	317
II.1	Kapitelzusammenfassung	317
II.2	Einführung	318
II.3	Ebenen des Monitorings	319

II.4	System Monitoring	321
II.4.1	Sicherheitsaspekte	322
II.4.2	Auswahl zu überwachender Systeme	322
II.4.3	Implementierung im Netzwerk	323
II.5	Protokoll-Monitoring	324
II.5.1	Unterstützung von Audits	325
II.5.2	Überwachung administrativer Tätigkeiten	325
I2	<b>IT-Security Audit</b>	327
I2.1	Kapitelzusammenfassung	327
I2.2	Einführung	328
I2.3	Audits im Kontext des IT-Security Managements	328
I2.4	Audits im Unternehmenskontext	331
I2.5	Audits nach Kategorien	332
I2.6	Vor-Ort kontra Selbstauskunft	334
I2.7	Anforderungen an den Auditor	335
I2.8	Ein Audit Schritt für Schritt	337
I2.8.1	Vorbereitung	338
I2.8.2	Durchführung	339
I2.8.3	Nachbereitung	343
I2.8.4	Abschlussbericht	344
I3	<b>Incident Response und IT-Forensik</b>	347
I3.1	Kapitelzusammenfassung	347
I3.2	Einführung	348
I3.3	Grundlagen der IT-Forensik	351
I3.3.1	Arten der IT-Forensik-Analyse	351
I3.3.2	Unterschiedliche Zielsetzungen	352
I3.4	Angriffe auf Ihre Daten	353
I3.4.1	Durch eigene Mitarbeiter	354

13.4.2	Durch Außenstehende	356
13.4.3	Angriffe und Angriffsvektoren	356
13.4.4	Angriffsarten	357
13.5	Elemente der forensischen Untersuchung	361
13.5.1	Zielsetzung	362
13.5.2	Anforderungen an die Analyse	363
13.5.3	Forensische Methoden	365
13.5.4	Forensische Untersuchung	366
<b>14</b>	<b>Kennzahlen</b>	<b>371</b>
14.1	Kapitelzusammenfassung	371
14.2	Einführung	372
14.3	Aufgabe von Kennzahlen	372
14.4	Quantifizierbare Kennzahlen	375
14.5	Steuerung mithilfe von Kennzahlen	377
14.6	Qualität von Kennzahlen	378
14.6.1	Gute Kennzahlen	378
14.6.2	Schlechte Kennzahlen	379
14.6.3	Vergleichbarkeit von Kennzahlen	379
14.7	Verschiedene Kennzahlen aus der IT-Security	380
14.8	Kennzahlen im laufenden Verbesserungsprozess	384
14.9	Laufende Auswertung von Kennzahlen	386
14.10	Annualized Loss Expectancy	386
14.11	IT-Security Balanced Scorecard	389
14.11.1	Einführung der IT-Security Balanced Scorecard	391
14.11.2	Maßnahmenziele für den Bereich IT-Security	395
<b>15</b>	<b>Praxis: Aufbau eines ISMS</b>	<b>399</b>
15.1	Kapitelzusammenfassung	399
15.2	Einführung	400

<b>15.3</b>	<b>ISMS in Kürze</b>	<b>401</b>
<b>15.4</b>	<b>Herangehensweise</b>	<b>403</b>
<b>15.5</b>	<b>Schritt für Schritt zum ISMS</b>	<b>405</b>
<b>15.5.1</b>	<b>Plan-Do-Check-Act</b>	<b>408</b>
<b>15.5.2</b>	<b>Vorarbeiten</b>	<b>410</b>
<b>15.5.3</b>	<b>Plan: Gestaltung des ISMS</b>	<b>414</b>
<b>15.5.4</b>	<b>Do: Umsetzung der Arbeitspakete</b>	<b>428</b>
<b>15.5.5</b>	<b>Check: Überprüfung des ISMS</b>	<b>430</b>
<b>15.5.6</b>	<b>Act: Umsetzung von erkannten Defiziten</b>	<b>430</b>
<b>15.5.7</b>	<b>Dokumentation</b>	<b>431</b>
<b>15.6</b>	<b>Softwaregestützter Aufbau eines ISMS</b>	<b>435</b>
<b>15.6.1</b>	<b>Auswahl einer ISMS-Lösung</b>	<b>437</b>
<b>15.6.2</b>	<b>Darstellung der Unternehmenswerte</b>	<b>439</b>
<b>15.6.3</b>	<b>Darstellung von Prozessen</b>	<b>441</b>
<b>15.6.4</b>	<b>IT-Risikomanagement</b>	<b>442</b>
<b>15.6.5</b>	<b>Richtlinienmanagement</b>	<b>445</b>
<b>15.6.6</b>	<b>Arbeitsabläufe abbilden</b>	<b>446</b>
<b>15.6.7</b>	<b>Berichte erstellen</b>	<b>447</b>
<b>15.7</b>	<b>Zertifizierung nach ISO 27001</b>	<b>447</b>
<b>15.7.1</b>	<b>Ansprechpartner</b>	<b>450</b>
<b>15.7.2</b>	<b>Prinzipien</b>	<b>450</b>
<b>16</b>	<b>Awareness und Schulung</b>	<b>453</b>
<b>16.1</b>	<b>Verbesserungsprozess</b>	<b>454</b>
<b>16.2</b>	<b>Voraussetzungen für eine Sicherheitskultur</b>	<b>455</b>
<b>16.3</b>	<b>Erfassung der Sicherheitskultur</b>	<b>457</b>
<b>16.4</b>	<b>Top-down-Ansatz</b>	<b>458</b>
<b>16.5</b>	<b>Awareness-Projekte</b>	<b>459</b>
<b>Index</b>		<b>463</b>