

Inhaltsverzeichnis

	Einleitung	15
1	Umfang und Aufgabe des IT-Security-Managements	19
1.1	Kapitelzusammenfassung	19
1.2	Einführung	19
1.3	Informationen und Daten	20
1.4	IT-Security-Management ist wichtig	22
1.5	Wie gefährdet sind die Unternehmensdaten	24
1.5.1	Sicht des Verfassungsschutzes	24
1.5.2	Öffentliche Wahrnehmung	25
1.5.3	Die eigene Wahrnehmung	27
1.6	Begrifflichkeiten	28
1.7	Selbstverständnis der IT-Security-Organisation	30
1.8	Grundregeln	33
1.9	Umfang des IT-Security-Managements	35
1.9.1	Pfeiler der IT-Security	37
1.9.2	Aufgaben des IT-Security-Managements	41
1.10	IT-Security zwischen Nutzen und Kosten	44
2	Organisation der IT-Security	47
2.1	Kapitelzusammenfassung	47
2.2	Einführung	47
2.3	Rollen innerhalb des IT-Security-Managements	48
2.3.1	Manager IT-Security	48
2.3.2	Unternehmensleitung	54
2.3.3	Weitere Rollen	54

2.4	Verankerung im Unternehmen	56
2.4.1	IT-Security im Organigramm	56
2.4.2	IT-Security und der Datenschutz	63
2.4.3	Zusammenspiel mit anderen Sicherheitsbereichen	64
3	IT-Compliance	69
3.1	Kapitelzusammenfassung	69
3.2	Einführung	71
3.3	Standards	75
3.3.1	ISO-2700x-Reihe	76
3.3.2	Standards des Bundesamts für Sicherheit in der Informationstechnik	82
3.3.3	Gegenüberstellung ISO 2700x und BSI-Grundschutz	87
3.3.4	ITIL	89
3.3.5	Weitere Standards	90
3.4	Gesetze	91
3.4.1	EU-Datenschutz-Grundverordnung	92
3.4.2	Weitere Gesetze	97
4	Organisation von Richtlinien	99
4.1	Kapitelzusammenfassung	99
4.2	Einführung	100
4.3	Strukturierung von Richtlinien	101
4.4	Beschreibung und Kategorisierung	102
4.5	Pflege und Lenkung von Richtlinien	103
4.6	Richtlinien und Audits	105
4.7	Verschiedene Richtlinien	107
4.7.1	Sicherheitsrichtlinie	108
4.7.2	Klassifizierungsrichtlinie	113
4.7.3	ISMS-Handbuch	116
4.7.4	Richtlinie zum IT-Risikomanagement	118
4.7.5	IT-Sicherheitsrichtlinie	120

4.7.6	IT-Systemrichtlinien	124
4.8	Von der Theorie in die Praxis	125
5	Betrieb der IT-Security	127
5.1	Kapitelzusammenfassung	127
5.2	Einführung	127
5.3	IT-Security und der IT-Betrieb	129
5.4	Betriebliche Grundsätze	130
5.4.1	Ableitung aus gesetzlichen Vorschriften	130
5.4.2	Vertragswesen	131
5.4.3	Administrative Tätigkeiten	131
5.4.4	Trennung von Funktionen	132
5.4.5	Prinzip der geringsten Rechte	133
5.5	IT-Security-Prozesse	134
5.5.1	Zugangs- und Zugriffskontrolle	134
5.5.2	Sicherheit von Software	141
5.5.3	Sichere Softwareentwicklung	146
5.5.4	Identitätsmanagement	148
5.5.5	Genehmigungsprozesse	153
5.5.6	Standardisierung	154
5.5.7	Unterstützung des IT-Betriebs	155
6	IT Business Continuity Management	157
6.1	Kapitelzusammenfassung	157
6.2	Einführung	158
6.3	Abgrenzung der Begriffe	162
6.4	IT-Notfallmanagement und Verfügbarkeitsmanagement	164
6.5	Gesetzliche Rahmenbedingungen des IT Business Continuity Managements	165
6.6	Business-Impact-Analyse	165
6.6.1	Erfassung und Priorisierung der Geschäftsprozesse	166

6.6.2	Business-Impact-Analyse in der Praxis	172
6.7	Weitere Einflussfaktoren	173
7	IT-Notfallmanagement	175
7.1	Kapitelzusammenfassung	175
7.2	Einführung	175
7.3	IT-Notfallmanagement	176
7.4	Richtlinie zum IT-Notfallmanagement	177
7.5	Ableitung von Notfallstrategien	178
7.6	IT-Notfallkonzepte erstellen	179
7.6.1	Schweregrade	181
7.6.2	Notfallvorsorge	183
7.7	Notfallorganisation	189
7.7.1	Organisationsstruktur	189
7.7.2	Kompetenzen und Zuständigkeiten	190
7.7.3	Notfallhandbuch	191
7.8	Notfallbewältigung	193
7.9	Notfallübungen	197
7.10	Überprüfung des IT-Notfallmanagements	198
7.11	Monitoring im Rahmen des IT Business Continuity Managements	199
7.12	Checklisten IT-Notfallmanagement	200
7.12.1	Checkliste Business-Impact-Analyse	200
7.12.2	Checkliste Notfallorganisation	201
7.12.3	Checkliste Notfallpläne und Wiederanlaufpläne	202
7.12.4	Checkliste Rechenzentrum	202
8	Verfügbarkeitsmanagement	205
8.1	Kapitelzusammenfassung	205
8.2	Einführung	205

8.3	Richtlinie zum Verfügbarkeitsmanagement	206
8.4	Verfügbarkeit	207
8.4.1	Klassifizierung von Verfügbarkeit	208
8.4.2	Vorgehensweise	210
8.4.3	Berechnung der Verfügbarkeit	211
8.5	Ausfallsicherheit	212
8.6	Ausprägungen von Redundanz	213
8.6.1	Strukturelle Redundanz	214
8.6.2	Funktionelle Redundanz oder unterstützende Redundanz	215
8.6.3	Informationsredundanz	215
8.7	Redundante Hard- und Software	215
8.8	Virtualisierung	217
8.9	Bauliche Maßnahmen zur Steigerung der Verfügbarkeit	218
9	Technische IT-Security	221
9.1	Kapitelzusammenfassung	221
9.2	Einführung	222
9.3	Technisch-Organisatorische Maßnahmen	224
9.3.1	Zugangskontrolle	226
9.3.2	Zugriffskontrolle	231
9.3.3	Übertragungskontrolle und Transportkontrolle	233
9.3.4	Eingabekontrolle	237
9.3.5	Verfügbarkeitskontrolle, Wiederherstellbarkeit und Zuverlässigkeit	238
9.3.6	Datenintegrität	239
9.4	Verschlüsselung	240
9.4.1	Begriffsbestimmungen	241
9.4.2	Symmetrische Verschlüsselungssysteme	242
9.4.3	Asymmetrische Verschlüsselungsverfahren	243
9.5	Cloud Computing	244
9.5.1	Dienstleistungen in der Cloud	248
9.5.2	Risikofaktoren	250

9.5.3	Datenschutzrechtliche Aspekte	257
9.5.4	Vertragliche Vereinbarungen	259
9.5.5	Sinnvolle Freigabeprozesse	260
9.6	Betrieb von Firewalls	262
9.6.1	Paketfilter und Application-Gateways	264
9.6.2	Firewall-Regelwerk	267
9.6.3	Internet-Proxyserver	269
9.7	Internetzugang und Nutzung von E-Mail	270
9.7.1	Risikofaktor E-Mail	271
9.7.2	Verschlüsselung von E-Mails	272
9.7.3	Risikofaktor Internetbrowser	273
9.8	Penetrationstests	274
9.9	Digitale Signatur	276
9.10	Intrusion-Detection-Systeme	278
9.11	Wireless LAN	280
10	IT-Risikomanagement	283
10.1	Kapitelzusammenfassung	283
10.2	Einführung	284
10.3	IT-Risikomanagement im Unternehmenskontext	284
10.4	Akzeptanz des IT-Risikomanagements	286
10.5	Operatives IT-Risikomanagement	287
10.5.1	Vorgehensweise	290
10.5.2	IT-Risikomanagementprozess	292
10.5.3	Übergeordnete Risikobetrachtung	294
10.5.4	Schwachstellen	297
10.5.5	Bedrohungen	300
10.5.6	Zusammenspiel von Bedrohungen, Schwachstellen und Maßnahmen	302
10.5.7	Verhältnismäßigkeit	304
10.6	Schutzbedarfsfeststellung	305
10.6.1	Schutzziele	305

10.6.2	Schutzstufen	308
10.6.3	Prinzipien	309
10.6.4	Feststellung des Schutzbedarfs	310
10.6.5	Veränderung des Schutzbedarfs	315
10.6.6	Widersprüchliche Schutzziele	316
10.6.7	Schadensklassen	316
10.6.8	Abbildung des Datenflusses	317
10.6.9	Entscheidungsfindung auf Basis des Schutzbedarfs	318
10.7	IT-Risikomanagement Prozess	320
10.7.1	Risiken identifizieren	320
10.7.2	Risikoermittlung	325
10.7.3	Risikobewertung	328
10.8	Quantitative Darstellung von Risiken	331
10.8.1	Grundlagen der Risikoberechnung	332
10.8.2	Risikoberechnung im Beispiel	334
10.8.3	Risikomatrix	336
10.8.4	Risikokatalog	338
10.9	Risikobehandlung	340
10.9.1	Risiko akzeptieren	342
10.9.2	Risiko reduzieren	343
10.9.3	Risiko vermeiden	344
10.9.4	Risiko auf Dritte verlagern	344
10.10	Maßnahmen definieren	345
10.10.1	Maßnahmentypen	346
10.10.2	Individuelle Maßnahmenkataloge	347
11	Sicherheitsmonitoring	349
11.1	Kapitelzusammenfassung	349
11.2	Einführung	350
11.3	Ebenen des Monitorings	352
11.4	System-Monitoring	353
11.4.1	Sicherheitsaspekte	354
11.4.2	Auswahl zu überwachender Systeme	355

11.4.3	Implementierung im Netzwerk	356
11.5	Protokoll-Monitoring	357
11.5.1	Unterstützung von Audits	358
11.5.2	Überwachung administrativer Tätigkeiten	359
12	IT-Security-Audit	361
12.1	Kapitelzusammenfassung	361
12.2	Einführung	362
12.3	Audits im Kontext des IT-Security-Managements	362
12.4	Audits im Unternehmenskontext	366
12.5	Audits nach Kategorien	367
12.6	Vor-Ort kontra Selbstauskunft	369
12.7	Anforderungen an den Auditor	370
12.8	Ein Audit Schritt für Schritt	372
12.8.1	Vorbereitung	373
12.8.2	Durchführung	374
12.8.3	Nachbereitung	378
12.8.4	Abschlussbericht	378
13	Management von Sicherheitsereignissen und IT-Forensik	383
13.1	Kapitelzusammenfassung	383
13.2	Einführung	384
13.3	Angriffe auf Ihre Daten	385
13.3.1	Durch eigene Mitarbeiter	386
13.3.2	Durch Außenstehende	388
13.3.3	Angriffe und Angriffsvektoren	388
13.3.4	Angriffsarten	389
13.4	Management von Sicherheitsereignissen	394
13.5	IT-Forensik	396
13.5.1	Arten der IT-Forensik-Analyse	401
13.5.2	Einrichtung von Honey pots	402

13.6	Elemente der forensischen Untersuchung	403
13.6.1	Zielsetzung	404
13.6.2	Anforderungen an die Analyse	405
13.6.3	Forensische Methoden	406
13.6.4	Forensische Untersuchung	407
14	Kennzahlen	413
14.1	Kapitelzusammenfassung	413
14.2	Einführung	414
14.3	Die Aufgabe von Kennzahlen	414
14.4	Quantifizierbare Kennzahlen	417
14.5	Steuerung mithilfe von Kennzahlen	419
14.6	Qualität von Kennzahlen	421
14.6.1	Gute Kennzahlen	421
14.6.2	Schlechte Kennzahlen	422
14.6.3	Vergleichbarkeit von Kennzahlen	422
14.7	Verschiedene Kennzahlen aus der IT-Security	423
14.8	Kennzahlen im laufenden Verbesserungsprozess	428
14.9	Laufende Auswertung von Kennzahlen	430
14.10	Annualized Loss Expectancy	430
14.11	IT-Security Balanced Scorecard	433
14.11.1	Einführung der IT-Security Balanced Scorecard	435
14.11.2	Maßnahmenziele für den Bereich IT-Security	439
15	Praxis: Aufbau eines ISMS	443
15.1	Kapitelzusammenfassung	443
15.2	Einführung	444
15.3	ISMS in Kürze	445
15.4	Herangehensweise	448
15.5	Schritt für Schritt zum ISMS	449
15.5.1	Plan-Do-Check-Act	453

15.5.2	Vorarbeiten	454
15.5.3	Plan: Gestaltung des ISMS	459
15.5.4	Do: Umsetzung der Arbeitspakete	474
15.5.5	Check: Überprüfung des ISMS	476
15.5.6	Act: Umsetzung von erkannten Defiziten	477
15.5.7	Dokumentation	477
15.6	Softwaregestützter Aufbau eines ISMS	482
15.6.1	Auswahl einer ISMS-Lösung	483
15.6.2	Darstellung der Risiken und der Unternehmenswerte	486
15.6.3	Darstellung von Prozessen	488
15.6.4	IT-Risikomanagement	489
15.6.5	Richtlinienmanagement	492
15.6.6	Arbeitsabläufe abbilden	493
15.6.7	Berichte erstellen	493
15.7	Zertifizierung nach ISO 27001	494
15.7.1	Ansprechpartner	497
15.7.2	Prinzipien	497
16	Awareness und Schulung	501
16.1	Kapitelzusammenfassung	501
16.2	Verbesserungsprozess	502
16.3	Voraussetzungen für eine Sicherheitskultur	503
16.4	Erfassung der Sicherheitskultur	505
16.5	Top-down-Ansatz	506
16.6	Awareness-Projekte	507
	Index	511