

Inhalt

Vorwort	XI
Über den Autor	XII
1 Stellenwert der Informationssicherheit	1
1.1 Das Wesen einer Information	2
1.2 Informationstechnik als Informationsinfrastruktur	4
1.3 Sicherheit als Erfolgsfaktor	5
1.4 Sicherheitsfunktionen im Unternehmen	6
1.5 Risikomanagement vs. IT-Sicherheit	7
2 Risiko und Sicherheit	9
2.1 Risiko	9
2.1.1 Begriffsbedeutung	9
2.1.2 Risiko und Gefahr	11
2.1.3 Deutungen des Risikobegriffs	12
2.1.4 Erkenntnisse über Risiken	12
2.2 Sicherheit	14
2.2.1 Sicherheitskriterien	15
2.2.2 Sicherheitsgrad	18
2.2.3 Sicherheitsstufen	19
2.2.4 Verhältnis zwischen Sicherheitsgrad und Aufwand	20
3 Entstehung und Auswirkungen von Risiken	21
3.1 Schwachstelle	21
3.2 Angriffspfad	22
3.3 Auslöser	22
3.4 Bedrohung	23
3.5 Sicherheitsrelevantes Ereignis	24
3.6 Risikoszenario	25
3.7 Auswirkungen	26
3.8 Beispiele für Schadensszenarien	28

4	Sicherheitsorganisation.....	33
4.1	Sicherheitsbereiche im Unternehmen.....	33
4.1.1	Physische Sicherheit.....	34
4.1.2	Arbeitsicherheit.....	35
4.1.3	Technische Sicherheit.....	35
4.1.4	Produktionssicherheit.....	35
4.1.5	Produktsicherheit.....	36
4.1.6	Informationssicherheit.....	36
4.1.7	Umweltschutz.....	37
4.1.8	Datenschutz.....	37
4.1.9	Revision.....	37
4.1.10	Finanzielle Sicherheit.....	37
4.1.11	Patentschutz.....	37
4.2	Sicherheitsrelevante Rollen.....	38
4.2.1	Information Risk Manager.....	38
4.2.2	Information Security Manager.....	38
4.2.3	Informationssicherheits-Beauftragter.....	38
4.2.4	IT-Sicherheitsbeauftragter.....	39
4.2.5	Datenschutzbeauftragter.....	39
4.2.6	IT-Manager.....	39
4.2.7	IT-Revisor.....	39
4.2.8	IT-Sicherheitsgremium.....	40
4.2.9	IT-Benutzersupport.....	40
4.3	Organisationsmodelle.....	40
4.3.1	Beispiel 1.....	41
4.3.2	Beispiel 2.....	42
4.3.3	Beispiel 3.....	42
4.3.4	Beispiel 4.....	43
4.3.5	Beispiel 5.....	44
4.4	Gestaltung einer Sicherheitsorganisation.....	45
5	Methodische Managementgrundlagen	47
5.1	Vier-Phasen-Managementkreislauf.....	47
5.2	Der Information Security Circle.....	49
5.3	Zusammenspiel zwischen Statik und Dynamik.....	52
5.4	Fragebogen und Interviews.....	53
5.4.1	Fragebogentechnik.....	53
5.4.2	Interviewtechnik.....	55
5.5	Moderation.....	60
5.5.1	Grundaussagen zur Moderation.....	61
5.5.2	Der Moderator.....	61
5.5.3	Vorbereitung einer Moderation.....	62
5.5.4	Moderationsfragen.....	63
5.5.5	Moderationsbeispiel.....	64
5.5.6	Abfrage von Informationen.....	66
5.6	Argumentation und Verhandlung.....	66

5.6.1	Diskussions- und Verhandlungspartner	66
5.6.2	Gesprächsatmosphäre	67
5.6.3	Argumente	68
5.6.4	Verhandlungsvorgehen	68
5.6.5	Vierstufen-Verhandlungsprinzip.....	69
5.7	Projektmanagement	71
5.7.1	Projektorganisation	72
5.7.2	Projektplanung.....	77
5.7.3	Vorgehensmodelle	78
5.7.4	Projektstadien	80
5.7.5	Projektcontrolling	81
5.7.6	Projekttipps.....	82
6	Sicherheit definieren und vorgeben.....	83
6.1	Von der Zielsetzung zur Umsetzung	83
6.1.1	Zielhierarchie.....	84
6.1.2	Zielformulierung.....	85
6.1.3	Umsetzungsplanung.....	86
6.2	Sicherheitsstrategien.....	86
6.2.1	Strategie der chinesischen Mauer	87
6.2.2	Strategie der Prozess-basierten Sicherheit	87
6.2.3	Sicherheit von innen nach außen	87
6.2.4	Sicherheit durch Eigentümerschaft.....	88
6.2.5	Auswahl der Strategie.....	88
6.3	Sicherheitspolitik.....	88
6.3.1	Sicherheitspolitik als politische Handlungsweise	89
6.3.2	Sicherheitspolitik als Regelwerk der Sicherheit.....	91
6.4	Vordefinierte Sicherheitsstandards	99
6.4.1	BSI Grundschutzhandbuch	100
6.4.2	BS 7799	101
6.4.3	COBIT	103
6.5	Business Impact-Analyse	107
6.6	Abhängigkeitsmatrix	110
6.7	Schutzbedarfsanalyse	110
7	Risiken erkennen und bewerten.....	113
7.1	Abgrenzung des Analyseobjekts.....	114
7.2	IST-Aufnahme	114
7.2.1	Sichten von Dokumentationen	114
7.2.2	Führen von Interviews zur IST-Aufnahme	115
7.3	Schwachstellenanalyse	116
7.4	Bedrohungsanalyse.....	117
7.5	Risikoszenarien	117
7.6	Darstellung der Risikosituation	117
7.7	Der Risikokorridor	119
7.8	Bewerten der Risikosituation und Risikopriorisierung	121

7.9	Risikoentscheidung und -priorisierung.....	121
7.10	Angemessene Schutzkonzepte.....	122
7.11	Risikoformel.....	123
7.11.1	Eintrittswahrscheinlichkeit	124
7.11.2	Schadenshöhe	127
7.11.3	Probleme der Risikoformel.....	129
7.12	FMEA	130
7.13	Projektbegleitende Risikoanalyse.....	132
8	Reporting.....	135
8.1	Strukturmodell des House of Security (HoS)	135
8.1.1	Schichten	137
8.1.2	Dimensionen.....	138
8.1.3	Betrachtungshorizont.....	139
8.1.4	Lebenszyklusphasen	141
8.1.5	Tiefe und Schärfe	143
8.2	Präsentation	143
8.2.1	Allgemeines zur Präsentation	143
8.2.2	Vorbereitung der Präsentation sinhalte	144
8.2.3	Visualisierung der Inhalte.....	145
8.2.4	Vorbereitung der Präsentationsveranstaltung	146
8.2.5	Durchführung der Präsentation	149
8.3	Risk Reporting mit der Balanced Scorecard.....	150
8.3.1	Die betriebswirtschaftliche Balanced Scorecard.....	151
8.3.2	Anwendung der BSC im Sicherheitsmanagement	153
8.4	Security Capability Maturity Model.....	154
8.4.1	Das Capability Maturity Model (CMM).....	155
8.4.2	Das Security Capability Maturity Model.....	156
8.5	Reporting mit dem Netzdiagramm	158
8.6	Security Landscape	159
9	Business Continuity.....	161
9.1	Ausgangssituation	162
9.2	Klassische Datensicherung.....	165
9.3	Datenspiegelung	167
9.4	RAID.....	169
9.5	Moderne Storage-Technologien	175
9.6	Replikation	177
9.7	Failover	181
9.8	Redundanz.....	182
9.9	Outsourcing.....	185
9.10	Fallback.....	185
10	Notfallmanagement	187
10.1	Notfallvorsorge	188
10.2	Erkennen des Notfalls	191

10.3	Notfallhandbuch	195
10.4	Notfallorganisation	196
10.5	Notfallverlauf	200
10.5.1	Sofortmaßnahmen	201
10.5.2	Notfallbeherrschung	203
10.5.3	Eskalation	205
10.5.4	Notbetrieb	207
10.5.5	Notfall-Recovery	208
10.5.6	Notfall-Ende und Nachbereitung	209
11	Der Mensch in der Informationssicherheit	211
11.1	Politische Arbeit des Security Managers	212
11.1.1	Formale Macht	212
11.1.2	Die Unternehmensebenen und der Security Manager	213
11.1.3	Informelle Macht	216
11.1.4	Standing	217
11.1.5	Konsequenzen für Sie als Information Security Manager	218
11.1.6	Netzwerke schaffen	219
11.2	Change Management	221
11.2.1	Aussagen der offenen Widerständler	222
11.2.2	Verdeckter Widerstand	222
11.2.3	Verhinderungsgründe	223
11.2.4	Verschiedene Reaktionsmuster	224
11.2.5	Ablauf der Veränderung	225
11.2.6	Handlungsstrategien	227
11.3	Information Security Awareness	230
11.3.1	Gründe und Argumente für fehlende Awareness	230
11.3.2	Einsichten des Information Security Managers	231
11.3.3	Die Awareness verbessern	232
11.4	User Security Standard	235
12	Incident Handling und IT-Forensik	239
12.1	Computerkriminalität	239
12.2	Erkennung von sicherheitsrelevanten Ereignissen	241
12.2.1	Angriffsablauf	241
12.2.2	Erkennung über Abweichungen	243
12.2.3	Weiterleiten des sicherheitsrelevanten Ereignisses	244
12.3	Beweissicherung	244
12.3.1	Den unveränderten Originalzustand sicherstellen	244
12.3.2	Probleme mit Zeitangaben	246
12.4	Forensische Untersuchung	247
12.5	Bewertung von sicherheitsrelevanten Ereignissen	248
12.6	Umgang mit den Verursachern	248
12.6.1	Innentäter	248
12.6.2	Außentäter	249
12.7	Eskalation von sicherheitsrelevanten Ereignissen	249

12.7.1	Eskalation an das Notfallmanagement	249
12.7.2	Einbeziehung von externen Ermittlungskräften	250
12.7.3	Einbindung sonstiger externer Kräfte	250

13 Informationssicherheit und externe Partner 251

13.1	Externe Partner	251
13.2	Informationsrisiken in externen Partnerschaften	252
13.3	Sicherheitsanforderungen für externe Partner	255
13.4	Security Service Level Agreements	258
13.5	Vertraulichkeitserklärungen	259
13.6	Datenschutz im Outsourcing	261

14 Rechtliche Einflüsse 265

14.1	KonTraG	265
14.1.1	Stellung des Vorstands	266
14.1.2	Maßnahmen nach KonTraG	267
14.1.3	Geforderte Eigenschaften des Früherkennungssystems	267
14.1.4	Prüfungen nach KonTraG	268
14.2	COSO-Framework	269
14.3	Combined Code	271
14.4	Sarbanes Oxley Act (SOX)	273
14.5	Bundesdatenschutzgesetz	276
14.5.1	Die Gesetzesgrundlage zu personenbezogenen Daten	277
14.5.2	Anwendbarkeit des BDSG	279
14.5.3	Der betriebliche Datenschutzbeauftragte	281
14.6	Arbeitsrechtliche Haftung	283
14.7	Sonstige Haftungsregelungen	286
14.8	ITK-Gesetze	287
14.8.1	IuKDG	288
14.8.2	Teledienstegesetz	289
14.8.3	Signaturgesetz	289
14.8.4	TDDSG	292
14.8.5	TKG	293
14.8.6	TDSV	295
14.8.7	TKÜV	297
14.9	GoBS	299

Literatur 301

Register 305