

IT Security managen

**DAS  
INHALTS-  
VERZEICHNIS**

» Hier geht's  
direkt  
zum Buch

# Inhalt

<b>Vorwort</b> .....	<b>XIII</b>
Der Autor .....	XIV
<b>1 Stellenwert der Informationssicherheit</b> .....	<b>1</b>
1.1 Das Wesen einer Information .....	2
1.2 Informationstechnik als Informationsinfrastruktur .....	4
1.3 Sicherheit als Erfolgsfaktor .....	5
1.4 Sicherheitsfunktionen im Unternehmen .....	7
1.5 Risikomanagement vs. IT-Sicherheit .....	7
<b>2 Risiko und Sicherheit</b> .....	<b>9</b>
2.1 Risiko .....	9
2.1.1 Begriffsbedeutung .....	10
2.1.2 Risiko und Gefahr .....	11
2.1.3 Deutungen des Risikobegriffs .....	12
2.1.4 Erkenntnisse über Risiken .....	13
2.2 Sicherheit .....	15
2.2.1 Sicherheitskriterien .....	15
2.2.2 Sicherheitsgrad .....	19
2.2.3 Sicherheitsstufen .....	20
2.2.4 Verhältnis zwischen Sicherheitsgrad und Aufwand .....	21

<b>3</b>	<b>Entstehung und Auswirkungen von Risiken</b>	<b>23</b>
3.1	Schwachstelle	23
3.2	Angriffspfad	24
3.3	Auslöser	25
3.4	Bedrohung	26
3.5	Sicherheitsrelevantes Ereignis	27
3.6	Risikoszenario	28
3.7	Auswirkungen	29
3.8	Beispiele für Schadensszenarien	31
<b>4</b>	<b>Sicherheitsorganisation</b>	<b>35</b>
4.1	Sicherheitsbereiche im Unternehmen	35
4.1.1	Physische Sicherheit	36
4.1.2	Arbeitssicherheit	37
4.1.3	Technische Sicherheit	37
4.1.4	Produktionssicherheit	38
4.1.5	Produktsicherheit	38
4.1.6	Informationssicherheit	39
4.1.7	Umweltschutz	39
4.1.8	Datenschutz	39
4.1.9	Revision	40
4.1.10	Finanzielle Sicherheit	40
4.1.11	Patentschutz	40
4.2	Rollen in der IT-Sicherheit	41
4.2.1	IRM/ITRM	41
4.2.2	ISM/ITSM	41
4.2.3	ISB	42
4.2.4	ITSB	42
4.2.5	DSB	42
4.2.6	ITM	43
4.2.7	IT-Revision	43
4.2.8	IT-Sicherheitsgremium	43
4.2.9	IT-Benutzersupport	44
4.3	Organisationsmodelle	44
4.3.1	Beispiel 1	45

4.3.2	Beispiel 2 .....	46
4.3.3	Beispiel 3 .....	47
4.3.4	Beispiel 4 .....	48
4.3.5	Beispiel 5 .....	49
4.4	Gestaltung einer Sicherheitsorganisation .....	50
<b>5</b>	<b>IT Security Policy .....</b>	<b>53</b>
5.1	Historie .....	54
5.2	Bedeutungen und Ausprägungen .....	55
5.2.1	IT Security Policy als Sammlung technischer Sicherheitsmaßnahmen .....	56
5.2.2	IT Security Policy als Liste generischer IT-Sicherheitsanforderungen .....	56
5.2.3	IT Security Policy mit Meta-Anforderungen .....	57
5.2.4	IT Security Policy als Grundsatzdokument .....	57
5.3	Bestandteile einer IT Security Policy .....	58
5.3.1	Gültigkeitsbereich bzw. Reichweite .....	58
5.3.2	Inkraftsetzung .....	59
5.3.3	Behandlung von Verstößen .....	60
5.3.4	Verständlichkeit und Eindeutigkeit .....	60
5.4	Koordinierung und Strukturierung .....	61
5.4.1	Policy-Hierarchie .....	61
5.4.2	Zentrale Koordinierung .....	69
5.4.3	Objektorientierte und verkettete Policies .....	70
5.5	Information Security Controls .....	71
5.5.1	Formulierung von Controls .....	72
5.5.2	Control Objective .....	78
5.5.3	Zielrichtung der Control-Aktivität .....	79
5.6	Policy Management .....	82
<b>6</b>	<b>Sicherheit definieren und vorgeben .....</b>	<b>85</b>
6.1	Ziele .....	87
6.2	IT-Sicherheitsstrategien .....	91
6.2.1	Strategie der chinesischen Mauer .....	91
6.2.2	Strategie der prozessbasierten Sicherheit .....	92
6.2.3	Sicherheit von innen nach außen .....	92

6.2.4	Sicherheit durch Eigentümerschaft .....	93
6.2.5	Auswahl der Strategie .....	93
6.3	IT-Sicherheitspolitik .....	94
6.4	Business-Impact-Analyse .....	96
6.5	Abhängigkeitsmatrix .....	100
6.6	Schutzbedarfsanalyse .....	100
6.6.1	Technikorientierte Schutzbedarfsanalyse .....	101
6.6.2	Informationsorientierte Schutzbedarfsanalyse .....	102
6.7	IT-Sicherheitsstandards .....	103
6.7.1	BSI-Grundschutz .....	104
6.7.2	ISO 27001 und 27002 .....	109
6.8	Vier-Phasen-Managementkreislauf .....	112
6.9	Der Information Security Circle .....	113
6.10	Zusammenspiel zwischen Statik und Dynamik .....	117
6.11	IT-/OT-Sicherheit .....	118
6.11.1	Erweiterter Sicherheitsbegriff .....	119
6.11.2	OT Security Norm IEC 62443 .....	120
6.11.3	Übergreifendes IT/OT-Sicherheitsmanagement .....	123
<b>7</b>	<b>Risiken erkennen und bewerten .....</b>	<b>125</b>
7.1	Definition und Abgrenzung des Analyseobjekts .....	126
7.2	Ist-Aufnahme .....	126
7.2.1	Sichten von Dokumentationen .....	127
7.2.2	Führen von Interviews zur Ist-Aufnahme .....	128
7.2.3	Erheben des Ist-Zustands mit Fragebögen .....	134
7.3	Schwachstellenanalyse .....	136
7.4	Bedrohungsanalyse .....	138
7.4.1	Analyse der Bedrohungsfaktoren .....	138
7.4.2	Überprüfung vordefinierter potenzieller Bedrohungen .....	141
7.5	Risikoszenarien .....	142
7.6	Risikobewertung mit der Risikoformel .....	142
7.6.1	Eintrittswahrscheinlichkeit .....	143
7.6.2	Schadenshöhe .....	146
7.6.3	Probleme der Risikoformel .....	148
7.7	Darstellung der Risikosituation .....	149

7.8	Der Risikokorridor .....	151
7.9	Bewerten der Risikosituation und Risikopriorisierung .....	153
7.10	Risikobehandlung .....	154
7.11	Angemessene Schutzkonzepte .....	156
7.12	FMEA .....	158
7.13	Projektbegleitende Risikoanalyse .....	160
<b>8</b>	<b>Reporting .....</b>	<b>163</b>
8.1	Strukturmodell für das IT-Sicherheitsmanagement .....	163
8.1.1	Architekturschichten .....	165
8.1.2	Dimensionen .....	167
8.1.3	Betrachtungsebenen .....	168
8.1.4	Lebenszyklusphasen .....	170
8.1.5	Tiefe und Schärfe .....	172
8.2	Risk Reporting mit der Balanced Scorecard .....	173
8.2.1	Die betriebswirtschaftliche Balanced Scorecard .....	174
8.2.2	Anwendung der BSC im Sicherheitsmanagement .....	176
8.3	Security Capability Maturity Model .....	178
8.3.1	Das Capability Maturity Model (CMM) .....	178
8.3.2	Das Security Capability Maturity Model .....	180
8.4	Reporting mit dem Netzdiagramm .....	182
8.5	Security Landscape .....	182
<b>9</b>	<b>Business Continuity .....</b>	<b>185</b>
9.1	Ausgangssituation .....	187
9.2	Klassische Datensicherung .....	189
9.3	Datenspiegelung .....	192
9.4	RAID .....	194
9.5	Storage-Technologien .....	201
9.6	Replikation .....	203
9.7	Failover .....	207
9.8	Redundanz .....	208
9.9	Outsourcing .....	211
9.10	Fallback .....	212

<b>10</b>	<b>Notfallmanagement</b>	<b>215</b>
10.1	Notfallvorsorge	216
10.2	Notfallplanung	217
10.3	Erkennen des Notfalls	221
10.4	Notfallhandbuch	224
10.5	Notfallorganisation	226
10.6	Notfallverlauf	230
10.6.1	Sofortmaßnahmen	231
10.6.2	Notfallbeherrschung	234
10.6.3	Eskalation	236
10.6.4	Notbetrieb	238
10.6.5	Notfall-Recovery	239
10.6.6	Notfallende und Nachbereitung	241
<b>11</b>	<b>Der Mensch in der Informationssicherheit</b>	<b>243</b>
11.1	Politisches Wirken im IT-Sicherheitsmanagement	244
11.1.1	Formale Macht	244
11.1.2	Unternehmensebenen	246
11.1.3	Informelle Macht	248
11.1.4	Standing	249
11.1.5	Die Konsequenzen	251
11.1.6	Netzwerke schaffen	251
11.2	Change Management	254
11.2.1	Offener Widerstand	254
11.2.2	Verdeckter Widerstand	255
11.2.3	Verhinderungsgründe	256
11.2.4	Verschiedene Reaktionsmuster	257
11.2.5	Ablauf der Veränderung	259
11.2.6	Handlungsstrategien	260
11.3	Information Security Awareness	263
11.3.1	Gründe und Argumente für fehlende Awareness	263
11.3.2	Einsichten zum Leben der IT-Sicherheit	265
11.3.3	Die Awareness verbessern	266
11.4	User Security Standard	268

<b>12</b>	<b>Incident Handling und IT-Forensik</b>	<b>271</b>
12.1	Computerkriminalität	271
12.2	Erkennung von sicherheitsrelevanten Ereignissen	273
12.2.1	Ablauf eines möglichen Angriffs	273
12.2.2	Erkennung über Abweichungen	276
12.2.3	Weiterleiten des sicherheitsrelevanten Ereignisses	277
12.3	Beweissicherung	277
12.3.1	Den unveränderten Originalzustand sicherstellen	277
12.3.2	Probleme mit Zeitangaben	279
12.4	Forensische Untersuchung	280
12.5	Bewertung von sicherheitsrelevanten Ereignissen	281
12.6	Umgang mit der verursachenden Person	282
12.6.1	Interne Personen	282
12.6.2	Externe Personen	283
12.7	Eskalation von sicherheitsrelevanten Ereignissen	283
12.7.1	Eskalation an das Notfallmanagement	283
12.7.2	Einbeziehung von externen Ermittlungskräften	284
12.7.3	Einbindung sonstiger externer Kräfte	284
<b>13</b>	<b>IT-Sicherheit und externe Partner</b>	<b>285</b>
13.1	Externe Partner	286
13.2	Informationssicherheitsrisiken	286
13.3	Sicherheitsanforderungen für externe Partner	289
13.4	Security Service Level Agreements	293
13.5	Vertraulichkeitserklärungen	294
13.6	Datenschutz im Outsourcing	297
<b>14</b>	<b>Rechtliche Einflüsse</b>	<b>299</b>
14.1	IT-Sicherheitsgesetz	300
14.2	Datenschutz	302
14.2.1	Anwendbarkeit des Datenschutzes	303
14.2.2	EU Datenschutz-Grundverordnung (DSGVO)	305
14.2.3	Bundesdatenschutzgesetz (neu)	306
14.2.4	Der/die betriebliche Datenschutzbeauftragte	308
14.3	EU Cybersecurity Act	309



14.4	KonTraG .....	310
14.4.1	Stellung des Vorstands .....	311
14.4.2	Maßnahmen nach KonTraG .....	312
14.4.3	Geforderte Eigenschaften des Früherkennungssystems .....	313
14.4.4	Prüfungen nach KonTraG .....	314
14.5	COSO-Framework .....	315
14.6	UK Corporate Governance Code .....	318
14.7	Sarbanes-Oxley Act (SOX) .....	319
14.8	EU-Richtlinie 2006/43/EG („EuroSOX“) .....	322
14.9	Arbeitsrechtliche Haftung .....	323
14.10	Sonstige Haftungsregelungen .....	326
14.11	ITK-Gesetze .....	327
14.11.1	Informations- und Kommunikationsdienstegesetz (IuKDG) .....	328
14.11.2	Telemediengesetz (TMG) und Digitale-Dienste-Gesetz (DDG) .....	328
14.11.3	Signaturgesetz .....	330
14.11.4	Telekommunikationsgesetz (TKG) .....	330
14.11.5	Datenschutzgesetzgebung im ITK-Bereich .....	331
14.12	GoBS und GoBD .....	332
	<b>Literatur</b> .....	<b>335</b>
	<b>Index</b> .....	<b>339</b>