

Inhaltsverzeichnis

1 · Zur Motivation und Einführung	1
1.1 Management-Prozess	1
1.2 Verantwortlichkeit	2
1.3 Umfang	2
1.4 Betrachtungsebene	3
1.5 Vorgehensmodell	4
1.6 ISO 27000	4
1.7 IT-Grundschutz	5
1.8 Mentalitäten	5
1.9 Ganzheitliches Vorgehen?	5
1.10 Erfahrungen	6
2 Inventarisierung	9
2.1 „Inventar“ der Begriffe	9
2.2 Organisation und Rollen	10
2.3 Geschäfts- und Verwaltungsprozesse	18
2.4 IT-Anwendungen	23
2.5 Information und Daten	27
2.6 IT-Systeme	32
2.7 Netzwerk	35
2.8 Infrastruktur	37
2.9 Zusammenfassung	39
Literatur	40
3 Wesentliche Elemente des Sicherheitsprozesses	41
3.1 Die kontinuierliche Verbesserung	41
3.2 Unverzichtbar: Sensibilisierung, Schulung, Training	49
3.3 Lenkung der Dokumentation	52
3.4 Steuerung der Aufzeichnungen	56
3.5 Interne Audits	57

3.6	Die Management-Bewertung	58
3.7	Grundsätzliches zum Compliance Management	59
	Literatur	61
4	Sicherheitsziele auf allen Ebenen	63
4.1	Informationen und Daten	63
4.2	IT-Systeme	72
4.3	Geschäftsprozesse	76
5	Analysen	79
5.1	Analyse nach IT-Grundschutz	80
5.2	Die Schwachstellenanalyse	86
5.3	Ein Ansatz auf der Basis der ISO 15408	88
5.4	Risikoanalyse nach ISO/IEC 13335-3	98
5.5	Betrachtungsmodell der ISO 27005	108
5.6	Restrisiken und ihre Behandlung	116
	Literatur	117
6	Die Sicherheitsleitlinie	119
6.1	Inhalte der Sicherheitsleitlinie	120
6.2	Management der Sicherheitsleitlinie	124
	Literatur	126
7	Grundsätzliches zu Sicherheitsmaßnahmen	127
7.1	Maßnahmenklassen	127
7.2	Validierung von Maßnahmen	129
	Literatur	132
8	Das Sicherheitskonzept	133
8.1	Grundsätzliches	133
8.2	Sicherheitskonzept nach IT-Grundschutz	135
8.3	Klassisches IT-Sicherheitskonzept	136
8.4	Sicherheitskonzept nach ISO 27001	149
	Literatur	154
9	Rechtliche Sicherheit	155
9.1	Befolgen von Gesetzen	156
9.2	Vermeidung von Strafprozessen	160
9.3	Outsourcing	160
9.4	Verschiedenes	163

10 Organisatorische Maßnahmen	167
10.1 Vorgaben für die Abwicklung von Geschäftsprozessen	167
10.2 Festlegen von Rollen und Organisationsplänen	168
10.3 Organisatorische Anweisungen	169
11 Personelle Sicherheit	173
11.1 Arbeitsverträge	174
11.2 Vertrauliche Personaldaten	176
11.3 Verantwortung der Mitarbeiter für die Informationssicherheit	178
11.4 Personalmanagement	181
11.5 Ausscheiden von Mitarbeitern	181
11.6 Verschiedenes	182
12 Verhinderung unerwünschten Datenabflusses	183
12.1 Definitionen	184
12.2 Sensible Daten	184
12.3 Arten von Data Leakage	185
12.4 Rechtliche Maßnahmen	188
12.5 Organisatorische Maßnahmen	191
12.6 Data Leakage Protection in der Praxis	193
12.7 Zusammenfassung	197
13 Technische Sicherheitsmaßnahmen	199
13.1 Wahrung der Vertraulichkeit	199
13.2 Identifizierung und Authentisierung	200
13.3 Zugriffskontrolle	204
13.4 Wiederaufbereitung	209
13.5 Verschlüsselung	211
13.6 Wahrung der Integrität	219
13.7 Elektronische Signatur	222
13.8 Verfügbarkeit von Daten	230
13.9 System-Verfügbarkeit	233
13.10 Übertragungssicherung	239
13.11 Beweissicherung und Auswertung	240
Literatur	242
14 Sicherheit im Internet	243
14.1 Gefährdungen	244
14.2 Schutzmaßnahmen: Regelwerke für Internet und Email	246
14.3 Technische Schutzmaßnahmen: Internet-Firewalls	247
14.4 Zusammenfassung	252

15	Infrastruktursicherheit	253
15.1	Geltungsbereiche und Schutzziele	253
15.2	Gebäude, Fenster, Türen	254
15.3	Verkabelung	255
15.4	Drahtlose Netzwerke	256
15.5	802.11x WLAN (Wireless LAN)	257
15.6	Wi-Fi Protected Access (WPA/WPA2)	258
15.7	Weitere Infrastrukturprobleme und -maßnahmen	259
15.8	Richtlinien zur Zutrittskontrolle	262
15.9	Verfahren der Zutrittskontrolle	263
	Literatur	265
16	Sicherheitsmanagement – die tägliche Praxis	267
16.1	Aufrechterhaltung der Sicherheit	267
16.2	Messen der Sicherheit	269
16.3	Management von Sicherheitsvorfällen	271
16.4	Berichtswesen	274
	Literatur	275
17	IT Compliance	277
17.1	Unternehmensstrategie	277
17.2	Compliance als essentieller Bestandteil der IT-Strategie	278
17.3	Compliance und Risikomanagement	280
	Literatur	281
18	Zum Schluss...	283
	Literatur	286
	Fachbegriffe englisch./. deutsch	287
	Sachwortverzeichnis	289