

Inhaltsverzeichnis

Einleitung	19
Check-In	20
Einführung	24
I Praxis des Sicherheitsmanagements	33
Ziel I.01 Verantwortlichkeiten des Managements	34
Ziel I.02 Risikomanagement	35
I.2.1 Risikoanalyse	36
Bedrohungspotenzial	37
Ziel I.03 Ziel I.04 Kontrollmechanismen für die Sicherheit	40
Ziel I.05 Risikoberechnung	42
I.5.1 Quantitative und qualitative Ansätze	43
I.5.2 Umgang mit Risiken	46
I.5.3 Auswahl der Gegenmaßnahmen	47
Ziel I.06 Sicherheitspolitik und unterstützende Dokumente	47
I.6.1 Sicherheitspolitik	48
I.6.2 Normen	48
I.6.3 Mindestanforderungen	49
I.6.4 Verfahren	49
I.6.5 Leitlinien	49
Ziel I.07 Rollen und Verantwortlichkeiten	50
I.7.1 Dateneigentümer	50
I.7.2 Datenmanager	51
I.7.3 Anwender	51
I.7.4 Sicherheitsprüfer	51
Ziel I.08 Klassifikation von Informationen	52
I.8.1 Militärische und kommerzielle Klassifikationen	53
Ziel I.09 Personalmanagement	55
I.9.1 Administrative Kontrollen im Betrieb	56
I.10 Zwischenstation	57
I.11 Musterfragen	59
I.12 Musterantworten	63

2	Zugriffskontrolle	65
Ziel 2.01	Identifikation und Authentisierung	66
2.1.1	Definitionen	66
2.1.2	Drei Schritte zur Zugriffskontrolle	66
2.1.3	Authentisierung	67
	Biometrie	68
	Arten biometrischer Erkennung	69
	Kennwörter	71
	Wissensbasierte Kennwörter	73
	Einmalkennwörter	74
	Kryptographische Schlüssel	76
	Kennsätze	76
	Speicherkarten	76
	Smart Cards	77
2.1.4	Autorisierung	78
Ziel 2.02	Single-Sign-On-Technologien	79
2.2.1	Verzeichnisdienste	80
2.2.2	Kerberos	81
2.2.3	SESAME	84
2.2.4	Thin Clients	84
	Zugriffskontrollmodelle und Techniken	86
2.3.1	Offene (DAC-) Modelle	86
Ziel 2.03	2.3.2 Geschlossene (MAC-) Modelle	88
2.3.3	Rollenbasierte (RBAC-) Modelle	89
2.3.4	Zugriffskontrolltechniken	89
	Eingeschränkte Anwenderschnittstellen	90
	Zugriffs- und Berechtigungslisten	91
	Inhaltsabhängige Zugriffskontrolle	92
	Andere Techniken der Zugriffskontrolle	93
Ziel 2.04	Zugriffskontrollverwaltung	94
2.4.1	Zentrale Zugriffskontrollverwaltung	94
	RADIUS	94
	TACACS+	96
	Diameter	96
2.4.2	Dezentrale Zugriffskontrollverwaltung	96
Ziel 2.05	Intrusion-Detection-Systeme	97
2.5.1	Netzwerkbasierte und host-basierte Systeme	97
2.5.2	Signaturbasierte und verhaltensbasierte Systeme	98

2.5.3	Nachteile des IDS-Gedankens	100
2.5.4	Intrusion-Prevention-Systeme	100
Ziel 2.06	Kontrolle unberechtigter Zugriffe und Angriffe	101
2.6.1	Unberechtigte Offenlegung von Informationen	101
2.6.2	Elektromagnetische Emission und Sicherheit	103
2.6.3	Angriffstypen	104
2.6.4	Penetrationstests	106
2.6.5	Zwischenstation	107
2.7	Musterfragen	109
2.8	Musterantworten	113
3	Sicherheitsmodelle und Architekturen	115
Ziel 3.01	Systemkomponenten	115
3.1.1	Hauptprozessor	116
3.1.2	Speicherarten	119
	Virtueller Speicher	121
3.1.3	Speicherungsverfahren	123
3.1.4	Befehlsverarbeitung	123
3.1.5	Betriebszustände der Sicherheit	124
Ziel 3.02	Sicherheitsmechanismen des Betriebssystems	124
3.2.1	Prozessabtrennung	125
3.2.2	Schutzringe	125
3.2.3	Virtuelle Maschinen	127
3.2.4	Vertrauenswürdige Rechenumgebung (TCB)	128
3.2.5	Referenzmonitor und Sicherheitskernel	128
Ziel 3.03	Sicherheitsmodelle	129
3.3.1	Die Modelle	130
	Zustandsorientierte Maschine	130
	Bell-LaPadula-Modell	131
	Biba-Modell	133
	Clark-Wilson-Modell	135
	Das Modell von Goguen und Meseguer	136
	Zugriffskontrollmatrix-Modell	136
	Informationsflussmodell	136
	Chinesische Mauer	137
	Graham-Denning und Harrison-Ruzzo-Ullman-Modelle	138
	Evaluationskriterien der Sicherheit	140

Ziel 3.04	3.4.1	Sicherheitsevaluierungen	141
		Trusted Computer System Evaluation Criteria	141
		Die Regenbogen-Serie	143
		Information Technology Security Evaluation Criteria	143
		Common Criteria	144
	3.4.2	Zertifizierung und Akkreditierung	146
3.5		Zwischenstation	148
3.6		Musterfragen	149
3.7		Musterantworten	154
4	Physische Sicherheit		157
Ziel 4.01		Kontrollen in der physischen Sicherheit	157
	4.1.1	Standort	159
	4.1.2	Konstruktion und Bau der Anlagen	161
	4.1.3	Rechnerbereiche und Rechenzentren	165
	4.1.4	Hardware-Backups	166
Ziel 4.02		Stromversorgung und Umweltfragen	167
	4.2.1	Unterbrechungsfreie Stromversorgung (USV)	167
	4.2.2	Störungen	168
	4.2.3	Umweltfragen	171
	4.2.4	Belüftung	172
	4.2.5	Wasser, Dampf, Gas	173
Ziel 4.03		Brandschutz und Brandbekämpfung	173
	4.3.1	Vorbeugender Brandschutz	174
	4.3.2	Branderkennung	175
	4.3.3	Brandarten	177
	4.3.4	Brandbekämpfung	178
	4.3.5	Halon	179
	4.3.6	Fragen der Brandbekämpfung	179
	4.3.7	Sprinkleranlagen	180
	4.3.8	Krisenreaktion	181
Ziel 4.04		Sicherung der Außengrenzen	181
	4.4.1	Schlösser	182
	4.4.2	Zutritt zum Gelände	183
	4.4.3	Schutz des Eingangsbereichs	184
	4.4.4	Einfriedung	185
	4.4.5	Beleuchtung	186

4.5	4.4.6 Überwachungseinrichtungen	187
4.6	4.4.7 Einbruchmeldeanlagen	188
4.7	4.5 Zwischenstation	190
	4.6 Musterfragen	191
	4.7 Musterantworten	195
5	5 Sicherheit in Netzwerken und Telekommunikation	197
Ziel 5.01	TCP/IP-Protokoll	198
	5.1.1 Internet Protocol (IP)	200
	5.1.2 Netzwerke	201
	5.1.3 Intranets und Extranets	201
Ziel 5.02	Verkabelung und Datenübertragung	202
	5.2.1 Koaxialkabel	203
	5.2.2 Twisted-Pair-Kabel	204
	5.2.3 Glasfaser	205
	5.2.4 Verkabelungsprobleme	205
	5.2.5 Feuerfestigkeit	206
	5.2.6 Breitband- und Einzelband-Kabel	207
	5.2.7 Signale	207
	5.2.8 Asynchrone und synchrone Übertragung	208
	5.2.9 Übertragungsmethoden	208
Ziel 5.03	LAN-Technologien	209
	5.3.1 Netzwerktopologien	209
	5.3.2 Zugriffsmedien und Technologien	211
	Ethernet	212
	Token-Weitergabe	213
	Polling	213
	5.3.3 Protokolle	213
	Address Resolution Protocol (ARP)	213
	Reverse Address Resolution Protocol (RARP)	215
	Boot Protocol	216
	Internet Control Message Protocol (ICMP)	216
	Weitere Protokolle	216
Ziel 5.04	Netzwerkgeräte und Netzwerkdienste	217
	5.4.1 Repeater	218
	5.4.2 Bridge	218
	5.4.3 Switches	219
	VLAN	220

5.4.4	Router	220
5.4.5	Brouters	222
5.4.6	Gateways	222
5.4.7	Zusammenfassung der Geräte	223
5.4.8	Firewalls.	223
	Paketfilterung	224
	Proxy-Firewalls	225
	Zustandsorientierte Firewalls	227
5.4.9	Firewall-Architektur	228
	Firewall-Administration	231
5.4.10	Fernzugriff.	232
	PPP.	232
	SLIP	232
	PAP	232
	CHAP.	233
	EAP.	233
5.4.11	VPN	234
	PPTP	234
	L2TP.	235
	IPSec	235
5.4.12	Netzwerkdienste	236
	DNS	236
	NAT	237
Ziel 5.05	Telekommunikationsprotokolle und -dienste	238
5.5.1	FDDI	239
5.5.2	SONET.	239
5.5.3	Standleitungen	240
5.5.4	CSU/DSU	242
5.5.5	S/WAN.	242
5.5.6	Open/VPN.	242
5.5.7	ISDN	243
5.5.8	DSL.	244
5.5.9	Kabelmodems	245
5.5.10	WAN Switching.	246
5.5.11	Frame Relay.	247
5.5.12	X.25	248
5.5.13	ATM	248

5.5.14	Quality of Service	248
5.5.15	SMDS	249
5.5.16	SDLC	249
5.5.17	HDLC	250
5.5.18	Kombinierte Zugangstechnologien	250
Ziel 5.06	Methoden und Technologien des Fernzugriffs	250
5.6.1	Fernzugriff	251
5.6.2	Drahtlose Technologien	253
	Mehrfrequenzverfahren	253
	WAP	254
	Bluetooth	255
	Access Points	255
	SSID	256
	OSA und SKA	256
5.6.3	Klonen von Mobiltelefonen	258
5.6.4	Bedrohungen bei TK-Anlagen	259
Ziel 5.07	Fehlertolerante Mechanismen	260
5.7.1	RAID	261
5.7.2	Clustering	261
5.7.3	Backup	261
5.8	Zwischenstation	261
5.9	Musterfragen	263
5.10	Musterantworten	269
6	Kryptographie	273
Ziel 6.01	Definitionen in der Kryptographie	274
6.1.1	Definitionen	274
6.1.2	Schlüssel und Text	275
6.1.3	Schlüsselmenge	276
6.1.4	Stärke von Kryptosystemen	277
6.1.5	Angriffe	278
6.1.6	Scheinverfahren	279
6.1.7	Steganographie	280
Ziel 6.02	Verschlüsselungsverfahren	281
6.2.1	Das Kerckhoff-Prinzip	282
6.2.2	Schlüsselhinterlegung	283
6.2.3	Ersetzungsverfahren	285

6.2.4	Transpositionsverfahren.	285
6.2.5	Blockalgorithmen	285
6.2.6	Stromalgorithmen.	287
6.2.7	Symmetrische Kryptographie.	289
6.2.8	Asymmetrische Kryptographie.	291
Ziel 6.03	Hybride Ansätze	295
6.3.1	Schlüsselmanagement	296
6.3.2	Datenverschlüsselung.	298
6.3.3	Sicherheitsziele	298
6.3.4	Symmetrische Algorithmen.	299
	DES	299
	Triple-DES (3DES)	301
	Advanced Encryption Standard (AES)	302
6.3.5	Andere symmetrische Algorithmen	302
6.3.6	Asymmetrische Algorithmen.	303
	Der Schlüsselaustausch nach Diffie-Hellman	303
	El Gamal	304
	Kryptosysteme mit elliptischen Kurven (ECC)	304
Ziel 6.04	Nachrichtenintegrität und digitale Signaturen	304
6.4.1	Nachrichtenintegrität	304
	One-Way Hash	305
	Angriffe auf Hash-Funktionen	306
	Hashing-Algorithmen.	308
6.4.2	Nachrichtenauthentisierungscode.	308
6.4.3	Elektronische Unterschriften.	310
	DSS	311
Ziel 6.05	Kryptographische Anwendungen	312
6.5.1	Public Key Infrastructure (PKI)	312
	Zertifizierungsstelle	312
	Registrierungsstelle	313
	Widerruf von Zertifikaten	314
	PKI-Komponenten	314
	PKI-Schritte	315
6.5.2	Einmaltableau	316
6.5.3	Verschlüsselung auf mehreren Ebenen	318
Ziel 6.06	Kryptographische Protokolle	319
6.6.1	Privacy-Enhanced Mail (PEM)	320
6.6.2	Nachrichten-Sicherheitsprotokoll	321

6.6.3	Pretty Good Privacy (PGP)	321
6.6.4	Sicherheit im Internet	322
	Secure Hypertext Transfer Protocol (S-HTTP)	322
	HTTPS	322
	Secure Sockets Layer (SSL)	323
	S/MIME	323
	SSH	324
	SET	324
	IPSec	326
	Andere Sicherheitstechnologien	330
Ziel 6.07	Angriffe	330
6.7.1	Chiffertext-Angriff	330
6.7.2	Angriff bei bekanntem Klartext	331
6.7.3	Angriff auf ausgewählten Klartext	331
6.7.4	Adaptiver Angriff auf ausgewählten Klartext	331
6.7.5	Angriff auf ausgewählten Chiffertext	332
6.7.6	Adaptiver Angriff auf ausgewählten Chiffertext	332
6.7.7	Mittelsmann-Angriff	332
6.7.8	Algebraischer Angriff	332
6.7.9	Analytischer Angriff	332
6.8	Zwischenstation	333
6.9	Musterfragen	335
6.10	Musterantworten	339
7	Notfallplanung und betriebliches Kontinuitätsmanagement	341
Ziel 7.01	Notfallplanung im Gegensatz zur betrieblichen Kontinuität	343
Ziel 7.02	Projektinitialisierung	345
Ziel 7.03	Folgeschädenanalyse	347
Ziel 7.04	Mögliche Bedrohungen	352
Ziel 7.05	Backups und Ausweichmöglichkeiten	354
7.5.1	Mitarbeiter und Arbeitsumgebung	354
7.5.2	Auswahl eines Lagerorts für Backups	356
7.5.3	Alternative Backupmöglichkeiten	357
Ziel 7.06	Planungsziele der Notfall- und Kontinuitätsplanung	359
7.6.1	Krisenreaktion	362
7.6.2	Wiederanlauf und Wiederherstellung	363
7.6.3	Dokumentation	364
7.6.4	Tests und Übungen	364

7.6.5	Wartung	366
7.6.6	Phaseneinteilung	367
7.6.7	Prävention	367
7.7	Zwischenstation	368
7.8	Musterfragen	369
7.9	Musterantworten	374
8	Recht, Ermittlungen und Ethik	377
Ziel 8.01	Ethik	378
8.1.1	(ISC)2	378
8.1.2	Computer Ethics Institute	379
8.1.3	Internet Activities Board	379
Ziel 8.02	Hacking-Methoden	380
8.2.1	Eigenschaften der Angreifer	381
8.2.2	Schwierigkeiten bei der Strafverfolgung	383
8.2.3	Angriffstypen	384
	Salami	384
	Datenverfälschung	384
	Übermäßige Sonderrechte	384
	Ausspähen von Kennwörtern	385
	IP Spoofing	385
	Mistwühler	385
	Anzapfen	386
	Social Engineering	386
8.2.4	Andere Angriffstypen	387
8.2.5	Angriffsategorien	387
8.2.6	Telefonbetrug	388
	Organisatorische Haftung und ihre Auswirkungen	389
8.3.1	Sicherheitsprinzipien	389
Ziel 8.03	8.3.2 Gesetzliche Haftung	390
8.3.3	Schutz der Privatsphäre	390
	Privacy Act 1974	390
	Electronic Communications Privacy Act 1986	391
	Health Insurance Portability and Accountability Act (HIPAA)	391
	Gramm Leach Bliley Act 1999	391
	Überwachung der Mitarbeiter	392
	Grenzüberschreitender Datenverkehr	393

8.3.4	Internationale Fragen	394
	Rechtsvorschriften	395
8.4.1	Zivilrecht	395
8.4.2	Strafrecht	395
Ziel 8.04	8.4.3 Verwaltungsrecht	396
	8.4.4 Bundesgesetze	396
	Computer Fraud and Abuse Act 1986	397
	Economic Espionage Act 1996	397
	Federal Sentencing Guidelines 1991	397
	8.4.5 Urheberrecht	397
	Geschäftsgeheimnisse	398
	Copyright	398
	Warenzeichen	399
	Patent	399
	8.4.6 Softwarepiraterie	400
Ziel 8.05	Ermittlungen und Computerkriminalität	401
8.5.1	Wer ermittelt?	401
8.5.2	Reaktion auf Vorfälle	402
8.5.3	Incident Response Team	403
8.5.4	Handhabung von Vorfällen	403
8.5.5	Beweisaufnahme	404
8.5.6	Durchsuchung und Beschlagnahme	406
8.5.7	Forensische Prüfung	406
8.5.8	Zulässigkeit von Beweisen	407
8.5.9	Arten von Beweisen	408
	Zwingende Beweise	408
	Sekundäre Beweise	408
	Hörensagen	409
8.5.10	Verleitung und Fallen	409
8.5.11	Verfahren	410
8.6	Zwischenstation	411
8.7	Musterfragen	412
8.8	Musterantworten	417
9	System- und Anwendungsentwicklung	421
Ziel 9.01	Projektentwicklung	422
9.1.1	Softwarelebenszyklus	423

9.1.2	Software-Entwicklungsmodelle	423
	Projektinitiation	424
	Funktionales Design, Analyse und Planung	424
	Systemdesign/Spezifikation	425
	Softwareentwicklung	425
	Akzeptanztest/Implementierung	426
	Betrieb und Wartung	427
	Entsorgung	427
9.1.3	Methoden der Softwareentwicklung	427
9.1.4	Änderungskontrolle	428
9.1.5	Administrative Kontrollen	429
9.1.6	Entwicklung der Programmiersprachen	430
Ziel 9.02	Objektorientierte Programmierung	431
	Klassen und Objekte	432
	Abstraktion	433
	Polymorphie	433
9.2.1	Polyinstantiation	433
9.2.2	Bedrohungen für Anwendungen	434
Ziel 9.03	Verteiltes Rechnen	436
9.3.1	ORB und CORBA	436
9.3.2	COM und DCOM	437
9.3.3	Enterprise Java Bean	438
9.3.4	OLE	438
9.3.5	ActiveX	439
9.3.6	Java-Applets	440
9.3.7	CGI	440
9.3.8	Cookies	441
	Datenbanken	442
9.4.1	Relationales Datenmodell	442
Ziel 9.04	Data Dictionary	444
	Datenbank-Jargon	444
	Structured Query Language	445
9.4.2	Hierarchisches Modell	446
9.4.3	Vernetztes Datenbankmanagement	446
9.4.4	Verteiltes Datenmodell	446
9.4.5	Objektorientierte Datenbanken	446
9.4.6	Datenbank-Interfacesprachen	447

9.4.7	Gleichzeitiger Zugriff	449
9.4.8	Aggregation und Rückschluss	450
9.4.9	Aggregation	452
9.4.10	Inferenz	452
9.4.11	Data Warehousing	452
	Data Mining	453
	Künstliche Intelligenz	454
9.5.1	Expertensysteme	454
Ziel 9.05	9.5.2 Neuronale Netze	455
Ziel 9.06	Malware	456
9.6.1	Viren	457
9.6.2	Würmer	458
9.6.3	Logische Bomben	458
9.6.4	Trojanische Pferde	458
9.6.5	Denial of Service	459
9.6.6	Distributed Denial of Service	459
9.6.7	Smurf-Angriffe	460
9.6.8	Timing-Angriffe	460
9.6.9	Rootkits	461
9.6.10	Botnets	461
9.6.11	Spam	461
9.6.12	Phishing	461
9.6.13	Angriffe über Sonderzeichen	461
9.6.14	Zero-Day-Exploits	462
9.7	Zwischenstation	462
9.8	Musterfragen	464
9.9	Musterantworten	468
10	Betriebliche Sicherheit	471
Ziel 10.01	Betriebliche Kontrollen	471
10.1.1	Kaufmännische Sorgfalt	473
10.1.2	Administrative Kontrolle	473
	Pflichtentrennung	474
	Stellenrotation	475
	Prinzip der geringsten Berechtigung und minimales Wissen	475
	Zwangspause	476

	Fehlergrenzen	476
10.1.3	Kontrolltypen	476
Ziel 10.02	Konfigurationsmanagement und Datenträgerkontrolle	478
10.2.1	Datenträgerzugriffskontrollen	480
10.2.2	Verarbeitungskontrollen	482
Ziel 10.03	Handhabung von Vorfällen und Wiederanlauf	482
10.3.1	Sicherer Rückfall	483
10.3.2	Fax-Sicherheit	484
10.3.3	Betriebliche Verantwortlichkeiten	485
	Ungewöhnliche oder unerklärliche Vorkommnisse	485
	Abweichungen vom Standard	486
	Unerwartetes Hochfahren	486
10.3.4	Operatives Personal	487
Ziel 10.04	Software-Backups	488
10.4.1	Netzwerkverfügbarkeit	488
	RAID	488
10.4.2	Backups	491
	Kontinuitätsmanagement	492
	Zwischenstation	493
10.6	Musterfragen	493
10.7	Musterantworten	497
A	Anhang A	499
B	Karriere-Flugroute	501
	Stichwortverzeichnis	505