

Inhaltsübersicht

1	Aufgaben und Ziele der Informationssicherheit	1
2	Betriebswirtschaftliche Aspekte der Informationssicherheit	15
3	Informationssicherheit und rechtliche Anforderungen	33
4	Datenschutzrecht	91
5	Hackermethoden	149
6	ISO 27001 und ISO 27002	163
7	IT-Grundschutz	181
8	Sicherheitskonzept	197
9	Datenschutzkonzept	203
10	Physische Sicherheit	215
11	Grundlagen der Netzwerksicherheit	229
12	Firewalls	287
13	Kryptografie	301
14	Vertrauensmodelle und PKI-Komponenten	341
15	Virtual Private Networks	369
16	Sicherheit in mobilen Netzen	393
17	Authentifizierung und Berechtigungsmanagement	435
18	Betriebssystemsicherheit	473
19	Windows-Sicherheit	503
20	Unix-Sicherheit	543
21	Virtualisierung	587
22	Sicherheit von mobilen Endgeräten	597
23	Anwendungssicherheit	605
24	Technisches Löschen und Vernichten	621
25	Datenschutzrechtliches Löschkonzept	641
26	Awareness	655
27	Malware und Content Security	673
28	Intrusion Detection	699
29	Datensicherung	717
30	Incident-Management und Computer-Emergency- Response-Teams	729
31	Business-Continuity-Management	751
32	Cloud Security	781
	Anhang	791
	Übersicht zu Standards der Informationssicherheit	793
	Index	831
	Abkürzungen und Glossar	855

Inhaltsverzeichnis

1	Aufgaben und Ziele der Informationssicherheit	1
	Einleitung	1
1.1	Aufgaben und Anforderungen eines ISMS	2
1.1.1	Risikomanagement	2
1.1.2	Gefährdungen erkennen und bewerten	3
1.1.3	Angreifermodelle betrachten.....	4
1.1.4	Hauptursachen für Sicherheitsprobleme identifizieren	4
1.1.5	Sicherheitskonzept erstellen.....	5
1.1.6	Sicherheitsmaßnahmen überprüfen	7
1.2	Generische Sicherheitsziele	8
1.2.1	Vertraulichkeit	8
1.2.2	Integrität	9
1.2.3	Verfügbarkeit	10
1.2.4	Authentizität	11
1.2.5	Sicherheitsziele und Sicherheitskonzept	11
	Zusammenfassung	13
	Literatur	13
2	Betriebswirtschaftliche Aspekte der Informationssicherheit	15
	Einleitung	15
2.1	Risikomanagement.....	16
2.2	Quantitative Modelle	17
2.2.1	Kosten von Risiken	18
2.2.2	Kosten von Sicherheitsvorfällen	20
2.2.3	Kosten von Sicherheitsmaßnahmen.....	21
2.2.4	Das ROSI-Modell	21
2.2.5	Grenzen des ROSI-Ansatzes	23
2.2.6	Alternative quantitative Modelle	24
2.3	Qualitative Betrachtungen	26
2.3.1	Grenzen betriebswirtschaftlicher Betrachtungen	26
2.3.2	Wirtschaftlichkeit von Investitionsentscheidungen	27
2.3.3	Risikomatrix.....	27
2.3.4	Pareto-Prinzip.....	28
2.3.5	Erfahrungswerte – Best Practice	29
	Zusammenfassung	30
	Literatur	31

3 Informationssicherheit und rechtliche Anforderungen

33

	Einleitung	33
3.1	Informationssicherheit und Recht im Überblick	35
3.1.1	Risikomanagement als rechtliche Anforderung	36
3.1.2	Anforderungen aus dem Gesellschaftsrecht	38
3.1.3	Anforderungen aus dem Bankenrecht	42
3.1.4	Anforderungen aus dem Steuer- und Handelsrecht	48
3.1.5	Informationssicherheit für Kritische Infrastrukturen	50
3.2	Telekommunikationsrecht	57
3.2.1	Grundlagen zur Informationssicherheit im Telekommunikationsrecht	58
3.2.2	Anforderungen an Informationssicherheit im Telekommunikationsrecht	59
3.2.3	Durchsetzung von Informationssicherheit im Telekommunikationsrecht	60
3.3	Strafrecht	61
3.4	Verträge und Vertragsrecht	62
3.4.1	Anforderungen an Informationssicherheit in Verträgen und im Vertragsrecht	62
3.4.2	Durchsetzung von Informationssicherheit in Verträgen und im Vertragsrecht	64
3.5	Arbeitsrecht	65
3.5.1	Arbeitsrecht als Gestaltungsmittel der Informationssicherheit	66
3.5.2	Regelungen im Arbeitsverhältnis	66
3.5.3	Regelungen durch Betriebsvereinbarung	69
3.6	Regulierte Infrastrukturen	70
3.6.1	eIDAS-Verordnung	70
3.6.2	Rolle und Anforderungen an Vertrauensdiensteanbieter	73
3.6.3	Arten von elektronischen Signaturen	75
3.6.4	Anforderungen an die Erstellung qualifizierter Zertifikate	77
3.6.5	Rechtsfolgen und Beweisrecht beim Einsatz von Vertrauensdiensten	78
3.7	Rechtliche Grenzen für Sicherheitsmaßnahmen	80
3.7.1	Datenschutzrecht	80
3.7.2	Telekommunikationsrecht	84
3.7.3	Telemedienrecht	87
3.7.4	Betriebliche Mitbestimmung	87
	Zusammenfassung	88
	Literatur	89

	Einleitung	91
4.1	Ziele des Datenschutzrechts	91
4.1.1	Entwicklung des Datenschutzrechts	91
4.1.2	Anwendungsbereich und Begriffsbestimmungen	93
4.1.3	Sachlicher Anwendungsbereich	93
4.1.4	Personenbezogene Daten	93
4.1.5	Verarbeitung von Daten	94
4.1.6	Räumlicher Anwendungsbereich	94
4.1.7	Weitere Begriffsbestimmungen	95
4.1.8	Rechtsrahmen und Umsetzungsvorgaben	95
4.1.9	Datenschutzrechtliche Grundprinzipien	96
4.1.10	Datenschutzleitlinie	98
4.1.11	Zweck und Geltungsbereich	98
4.1.12	Datenschutzrichtlinie	99
4.1.13	Richtlinie zur Privatnutzung des betrieblichen Internets und E-Mail	99
4.1.14	Richtlinie für datenschutzrechtliche Anforderungen an IT-Projekte	100
4.1.15	Datenschutzimplementierung/Datenschutzmanagement- system (DSMS)	101
4.1.16	Datenschutzrichtlinien und arbeitsanweisungen	101
4.1.17	Datenschutzorganisation	101
4.1.18	Datenschutzkonzept	102
4.2	Verarbeitungstätigkeiten	102
4.2.1	Datenschutz-Folgenabschätzung (Art. 35 DSGVO)	102
4.2.2	Rollen-Berechtigungskonzept	103
4.2.3	Informationspflichten	104
4.2.4	Auftragsverarbeitung	105
4.2.5	Auftragsverarbeitungsvertrag	106
4.2.6	Grenzen der Auftragsverarbeitung	107
4.2.7	Technische und organisatorische Maßnahmen (TOM)	107
4.2.8	Gemeinsame Verantwortlichkeit	110
4.2.9	Drittstaatentransfer von personenbezogenen Daten	111
4.2.10	Angemessenheitsbeschluss (Art. 45 DSGVO)	111
4.2.11	Vorliegen geeigneter Garantien (Art. 46 DSGVO)	111
4.2.12	Standarddatenschutzklauseln der Kommission oder einer Aufsichtsbehörde	112
4.2.13	Löschregeln	113
4.3	Datenschutz-Vorgänge	113
4.3.1	Datenschutzverpflichtung	113
4.3.2	Datenschutzschulung	114
4.3.3	Betroffenenrechte	114
4.3.4	Auskunft	115

4.3.5	Auskunftsersuchen von Betroffenen	115
4.3.6	Auskunftsersuchen von Dritten sowie von Ämtern und Ermittlungsbehörden	115
4.3.7	Berichtigung	116
4.3.8	Löschung	116
4.3.9	Einschränkung	117
4.3.10	Datenübertragung	118
4.3.11	Widerspruch	118
4.3.12	Datenschutzvorfälle	118
4.3.13	Whistleblower-Richtlinie	119
4.3.14	Benennung des Datenschutzbeauftragten	120
4.3.15	Audits	121
4.3.16	Kontinuierliche Umsetzungsverpflichtung der Sicherheit der Verarbeitung	122
4.3.17	Datenschutzaudit	122
4.3.18	Self Assessment	123
4.3.19	Zertifizierung	123
4.4	Gesetz über digitale Dienste	124
4.5	Sicherheit der Verarbeitung zur Gewährleistung der Informationssicherheit	125
4.5.1	Durchsetzung von Informationssicherheit im Datenschutzrecht	126
4.6	Telemedien-Datenschutzrecht	127
4.6.1	Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG)	127
4.6.2	Grundlagen zum Telemedien-Datenschutzrecht	128
4.6.3	Anforderungen an Datenschutz im Telemedienrecht	129
4.6.4	Durchsetzung von Datenschutz im Telemedienrecht	130
4.6.5	Cookie-Banner	131
4.6.6	Einwilligung nach § 25 TTDSG/Art. 6 Abs. 1 lit. a DSGVO	132
4.6.7	Nudging und Dark Pattern	133
4.7	Telekommunikations-Datenschutzrecht	134
4.7.1	Anforderungen an Datenschutz im Telekommunikationsrecht	135
4.7.2	Durchsetzung von Datenschutz im Telekommunikationsrecht	136
4.8	Strafrecht	136
4.8.1	Grundlagen zu Datenschutz und Informationssicherheit im Strafrecht	137
4.8.2	Anforderungen an Informationssicherheit und Datenschutz im Strafrecht	140
4.8.3	Durchsetzung von Datenschutz und Informationssicherheit im Strafrecht	141
4.8.4	Schutz der Informations- und Datenverarbeitung durch Strafrecht	141

4.9	Arbeitsrecht	143
4.9.1	Regelungen im Arbeitsverhältnis	144
4.9.2	Datenschutz im Homeoffice	144
4.9.3	Durchsetzung von Datenschutzmaßnahmen im Arbeitsverhältnis	145
4.9.4	Haftung der Arbeitnehmer	145
4.9.5	Regelungen durch Betriebsvereinbarung	146
	Zusammenfassung	147

5 Hackermethoden 149

	Einleitung	149
5.1	Begriffsdefinition »Hacker«	149
5.2	Ursachen von Sicherheitsproblemen	149
5.2.1	SQL-Injection	150
5.2.2	Buffer Overflows	151
5.2.3	Motivation eines Angreifers	153
5.3	Vorgehensweise bei Penetrationstests	154
5.3.1	Informationsbeschaffung	154
5.3.2	Portscans	155
5.3.3	Automatische Überprüfungen	156
5.3.4	Manuelle Untersuchungen	157
5.3.5	Anwendung von Exploits	157
5.3.6	Schwachstellenverkettung und Lateral Movement	158
5.3.7	Social Engineering	158
5.4	Angriffswerkzeuge	158
5.4.1	Rootkits	160
5.4.2	Virus Construction Kits	160
5.4.3	Trojaner und Kryptotrojaner	160
5.4.4	PowerShell	162
	Zusammenfassung	162
	Literatur	162

6 ISO 27001 und ISO 27002 163

	Einleitung	163
6.1	Entstehungsgeschichte	163
6.2	Die Familie der ISO-27000-Standards	165

6.3	ISO 27001	167
6.3.1	Vorgehensweise und Anwendungen.....	167
6.3.2	Inhaltliche Elemente der ISO 27001	168
6.3.3	Notwendige Dokumentation.....	171
6.3.4	Prüfungs- und Zertifizierungsprozess.....	172
6.4	ISO 27002.....	173
	Zusammenfassung	178
	Literatur	179
7	IT-Grundschutz	181
	Einleitung	181
7.1	Historie	181
7.2	IT-Grundschutz – der Ansatz	182
7.3	IT-Grundschutz-Dokumente	183
7.3.1	BSI-Standard 200-1: Managementsysteme für Informationssicherheit	184
7.3.2	BSI-Standard 200-2: IT-Grundschutz-Vorgehensweise	186
7.3.3	BSI-Standard 200-3: Risikomanagement	193
7.3.4	BSI-Standard 100-4: Notfallmanagement	193
7.3.5	IT-Grundschutz-Kompendium	194
7.4	Tool-Unterstützung	194
7.5	ISO 27001-Zertifizierung auf Basis von IT-Grundschutz.....	195
	Zusammenfassung	196
	Literatur	196
8	Sicherheitskonzept	197
	Einleitung	197
8.1	Ziele eines Sicherheitskonzepts.....	197
8.2	Zentrale Aufgaben im Sicherheitskonzept	199
8.2.1	Berechtigte und Unberechtigte.....	200
8.2.2	Schwachstellen vermeiden	201
8.2.3	Identifikation von Unregelmäßigkeiten	201
8.2.4	Reaktionen auf Störfälle	202
	Zusammenfassung	202
	Literatur	202

9	Datenschutzkonzept	203
	Einleitung	203
9.1	Ziele des Datenschutzkonzepts	203
9.2	Zentrale Elemente eines Datenschutzkonzepts	204
9.2.1	Organisation	205
9.2.2	Regelungen	206
9.2.3	Prozesse	207
9.2.4	Verträge	208
9.2.5	Audits	210
9.2.6	Dokumentation	211
9.2.7	Vorlagen	212
9.3	Regelmäßige Überarbeitung	212
	Zusammenfassung	213
10	Physische Sicherheit	215
	Einleitung	215
10.1	Bedrohungen	215
10.2	Erhöhung der Gebäudesicherheit	216
10.2.1	Bewusste Standortwahl	216
10.2.2	Sichere bauliche Gestaltung	217
10.2.3	Schutzzonen	218
10.2.4	Rettungs- und Fluchtwege	221
10.3	Angemessene Überwachung	221
10.4	Monitoring und automatisierte Maßnahmensteuerung	222
10.5	Wirksamer Brandschutz	222
10.6	Stromversorgung	223
10.7	Physische Schutzmaßnahmen in externen Bereichen	224
10.7.1	Mobile Endgeräte	224
10.7.2	Häuslicher Arbeitsplatz	224
10.7.3	Datenträger	224
	Zusammenfassung	225
	Literatur	225

11	Grundlagen der Netzwerksicherheit	229
	Einleitung	229
11.1	Das OSI-Modell	229
11.1.1	Protokolle, Adressen und Ports	232
11.1.2	Bedrohungen	234
11.2	Das Internet Protocol	234
11.3	IPv4	236
11.3.1	Address Resolution Protocol – ARP	236
11.3.2	Bedrohungen gegen IPv4	238
11.4	IPv6	241
11.4.1	Unterschiede zwischen IPv6 und IPv4	241
11.4.2	Neighbor Discovery	245
11.4.3	Header-Erweiterungen	247
11.4.4	Fragmentierung	248
11.4.5	Privatsphäre	249
11.4.6	Netzwerk-Scans	251
11.4.7	Produkte und Implementierungen	252
11.4.8	Besonderheiten zur Tunnelung von IPv6	252
11.5	Multiprotocol Label Switching – MPLS	253
11.6	Transportprotokolle	254
11.6.1	Sicherheitsmechanismen in Transportprotokollen	255
11.6.2	Übersicht über verschiedene Transportprotokolle	258
11.7	Netzwerkmanagementprotokolle	259
11.7.1	Konfigurationsprotokolle	259
11.7.2	Auskunftsdienst DNS	262
11.7.3	Routing-Protokolle	266
11.7.4	Anmerkung zu verschiedenen Sicherheitsmechanismen der Protokolle	268
11.8	Sicherheitsmechanismen für Netzwerke	269
11.8.1	IEEE 802.1X	269
11.8.2	IPsec	271
11.8.3	SSL/TLS	272
11.8.4	Datagram Transport Layer Security – DTLS	274
11.8.5	Secure Shell – SSH	274
11.8.6	Überwachung des Netzwerkverkehrs	275
11.9	Netzarchitektur	276
11.9.1	Einteilung des Netzes in Zonen	276
11.9.2	Zugriffskontrolle auf Switchen	278
11.9.3	Virtuelle LANs	279
11.9.4	Network Address Translation	282
11.9.5	Software Defined Networking (SDN)	283

	Zusammenfassung	284
	Literatur	285
12	Firewalls	287
	Einleitung	287
12.1	Grundlagen von Firewalls	287
12.1.1	Absicherung von Firewalls	288
12.1.2	Regelwerk	288
12.2	Firewall-Typen	289
12.2.1	Paketfilter	290
12.2.2	Application Level Gateway	290
12.2.3	Stealth Gateway	291
12.2.4	Unified Threat Management (UTM)/Next-Generation Firewalls	292
12.3	Firewall-Architekturen	292
12.3.1	Einstufige Paketfilter-Architektur	292
12.3.2	Multi-Homed-Architektur	293
12.3.3	Demilitarisierte Zone	294
12.3.4	PAP-Firewall-Architekturen	296
12.4	Firewall-Konzepte	298
12.4.1	Anforderungsanalyse für den Firewall-Einsatz	298
12.4.2	Betriebliche Anforderungen für die Firewall-Konzeption	299
12.5	Grenzen von Firewalls	299
	Zusammenfassung	300
	Literatur	300
13	Kryptografie	301
	Einleitung	301
13.1	Vorgehensweise	302
13.2	Begriffsklärung	303
13.3	Angriffs- und Sicherheitsziele	304
13.3.1	Lesen von Daten – Vertraulichkeit	304
13.3.2	Ändern von Daten – Integrität	305
13.3.3	Wiedereinspielen von Daten – Frische	305
13.3.4	Vortäuschen einer Identität – Urheber-Authentizität	306
13.3.5	Abstreiten der Verantwortung – Nicht-Abstreitbarkeit	306
13.3.6	Weitere Angriffs- und Sicherheitsziele	306
13.4	Grundsätzliche Angriffsszenarien	307

13.5	Sichere Kanäle	308
13.5.1	Verschlüsselung	309
13.5.2	Chiffrierverfahren	310
13.5.3	Betriebsmodi	316
13.5.4	Integrität	320
13.5.5	Authentisierte Verschlüsselung	324
13.6	Herausforderung Schlüsselverteilung	325
13.6.1	Der direkte Weg	325
13.6.2	Indirekt über vertrauenswürdige Dritte	327
13.7	Asymmetrische Verfahren zur Schlüsselverteilung	328
13.7.1	Grundprinzipien asymmetrischer Verfahren	328
13.7.2	Schlüsseltransport	329
13.7.3	Schlüsselaustausch	330
13.8	Digitale Signaturen	331
13.8.1	Grundprinzipien digitaler Signaturen	331
13.8.2	Digitale Signaturen für die Nicht-Abstreitbarkeit	333
13.8.3	Digitale Signaturen für Zertifikate	334
13.9	Praktischer Einsatz	334
13.9.1	Schlüssel- und Hash-Wert-Längen	334
13.9.2	Proprietäre Verfahren	337
13.9.3	Proprietäre Implementierungen	337
13.9.4	Erzeugung von Zufallszahlen	338
	Zusammenfassung	339
	Literatur	339
14	Vertrauensmodelle und PKI-Komponenten	341
	Einleitung	341
14.1	Vertrauensmodelle	342
14.1.1	Web of Trust	342
14.1.2	Zentrales Modell der Public-Key-Infrastruktur	344
14.2	Public-Key-Infrastruktur	345
14.2.1	Zertifikate und CRLs	345
14.2.2	Zertifizierungshierarchien	347
14.2.3	Verifikation einer digitalen Signatur	348
14.2.4	Komponenten und Prozesse einer PKI	350
14.2.5	Policies für Public-Key-Infrastrukturen	357
14.3	Standards im Bereich PKI	358
14.3.1	X.509-Standard	358
14.3.2	PKIX-Standards	358
14.3.3	PKCS-Standards	359
14.3.4	Common-PKI-Spezifikationen	360

14.4	Verknüpfung von Public-Key-Infrastrukturen	361
14.5	Langzeitarchivierung	364
	Zusammenfassung	366
	Literatur	366
15	Virtual Private Networks	369
	Einleitung	369
15.1	VPN-Szenarien	370
15.1.1	Site-to-Site-VPN	370
15.1.2	End-to-Site-VPN	371
15.1.3	End-to-End-VPN	371
15.1.4	Protokollebenen von VPN und VPN-Tunnel	372
15.2	Technische Realisierung von VPNs	373
15.2.1	PPP, L2F und PPTP.....	373
15.2.2	Layer 2 Tunneling Protocol – L2TP.....	374
15.2.3	IP Security – IPsec	379
15.2.4	OpenVPN.....	387
15.2.5	WireGuard	390
15.3	Spezielle Risiken von VPNs	390
	Zusammenfassung	391
	Literatur	391
16	Sicherheit in mobilen Netzen	393
	Einleitung	393
16.1	Bedrohungen in mobilen Netzen	393
16.2	Wireless LAN	395
16.2.1	Entwicklung und Standardisierung	395
16.2.2	Netzarchitektur und Netzkomponenten.....	396
16.2.3	Sicherheitsverfahren	397
16.2.4	Empfohlene Sicherheitsmaßnahmen	402
16.3	Bluetooth.....	403
16.3.1	Entwicklung und Standardisierung	403
16.3.2	Netzarchitektur und -komponenten	405
16.3.3	Sicherheitsverfahren in Bluetooth	406
16.3.4	Bluetooth-Sicherheitsmechanismen im Detail	412
16.3.5	Bewertung der Sicherheitsmaßnahmen	416

16.4 Mobilfunk..... 418

16.4.1 GSM 418

16.4.2 GPRS..... 427

16.4.3 UMTS 428

16.4.4 LTE..... 432

Zusammenfassung 432

Literatur 432

17 Authentifizierung und Berechtigungsmanagement 435

Einleitung..... 435

17.1 Benutzer 436

17.2 Identität 436

17.3 Identifizierung..... 437

17.4 Authentifizierung..... 437

17.4.1 Authentifizierung durch Wissen 438

17.4.2 Authentifizierung durch Besitz 445

17.4.3 Authentifizierung durch Biometrie 448

17.4.4 Authentifizierung in verteilten Systemen..... 449

17.5 Autorisierung und Zugriffskontrolle 453

17.5.1 Zugriffsrechtematrix 455

17.5.2 Zugriffskontrolllisten 455

17.5.3 Capabilities..... 456

17.5.4 Rollenbasierte Zugriffskontrolle 456

17.5.5 Nachteile von Zugriffskontrollstrategien..... 457

17.6 Identitäts- und Berechtigungsmanagement..... 458

17.7 Single Sign-On..... 459

17.7.1 Unternehmensweites Single Sign-On 459

17.7.2 SSO für Web-Services 461

17.7.3 OpenID..... 464

17.7.4 OAuth 2.0..... 465

17.7.5 OpenID-Connect 466

17.7.6 SAML 466

17.7.7 Mozilla Persona 467

17.7.8 Sicherheit von SAML, OpenID, OAuth und
Mozilla Persona 470

Zusammenfassung 471

Literatur 471

18	Betriebssystemsicherheit	473
	Einleitung	473
18.1	Identität und Autorisierung	474
18.1.1	Benutzer, Benutzergruppen und Rollen	475
18.1.2	Ressourcen	476
18.1.3	Zugriffsrechte	476
18.1.4	Erweiterung von Rechten – privilegierte Aktionen	477
18.2	Systemzugang und Authentisierung	478
18.2.1	Sicherer lokaler Zugang	478
18.2.2	Sicherer Fernzugang	478
18.2.3	Session-Sicherheit	485
18.3	Schutz der Anwenderdaten	486
18.3.1	Ablage auf Speichermedien	486
18.3.2	Verarbeitung im Speicher	488
18.3.3	Transit über ein Netzwerk	489
18.4	Konfigurationsmanagement	489
18.5	Protokollierung und Überwachung	490
18.5.1	Protokollierung und Auswertung	490
18.5.2	Überwachung im laufenden Betrieb	492
18.6	Selbstschutz und Härtung des Betriebssystems	493
18.6.1	Härtung gegen spezifische Bedrohungen	493
18.6.2	Malwareschutz	496
18.6.3	Boot-Schutz	498
18.6.4	Verwaltung angeschlossener Geräte und Speichermedien	499
18.6.5	Reduktion der Angriffsfläche	500
18.6.6	Einschränkung des zulässigen Netzwerkverkehrs	501
	Zusammenfassung	502
	Literatur	502
19	Windows-Sicherheit	503
	Einleitung	503
19.1	Identifizierung und Autorisierung	504
19.1.1	Benutzer, Benutzergruppen und Rollen	504
19.1.2	Ressourcen	507
19.1.3	Zugriffsrechte	511
19.1.4	Erweiterung von Rechten – privilegierte Aktionen	514
19.2	Systemzugang und Authentisierung	517
19.2.1	Sicherer lokaler Zugang	517
19.2.2	Sicherer Fernzugang	518
19.2.3	Session-Sicherheit	523

19.3	Schutz der Anwenderdaten	523
19.3.1	Ablage auf Speichermedien.....	523
19.3.2	Verarbeitung im Speicher.....	524
19.3.3	Transit über ein Netzwerk.....	524
19.4	Konfigurationsmanagement.....	525
19.4.1	Die Registry	525
19.4.2	Active Directory Domain Services	526
19.4.3	Gruppenrichtlinien	527
19.4.4	Management-Werkzeuge	527
19.5	Protokollierung und Überwachung	528
19.5.1	Protokollierung und Auswertung der Protokollierung.....	528
19.5.2	Überwachung im laufenden Betrieb	534
19.6	Selbstschutz und Härtung des Betriebssystems.....	535
19.6.1	Härtung gegen spezifische Bedrohungen	535
19.6.2	Malwareschutz.....	536
19.6.3	Bootschutz.....	538
19.6.4	Verwaltung angeschlossener Geräte und Speichermedien	538
19.6.5	Reduktion der Angriffsoberfläche.....	539
19.6.6	Einschränkung des zulässigen Netzwerkverkehrs.....	539
	Zusammenfassung	540
	Literatur	540
20	Unix-Sicherheit	543
	Einleitung.....	543
20.1	Identität und Autorisierung	544
20.1.1	Benutzer, Benutzergruppen und Rollen	544
20.1.2	Ressourcen.....	549
20.1.3	Zugriffsrechte	555
20.1.4	Erweiterung von Rechten – privilegierte Aktionen	563
20.2	Systemzugang und Authentisierung	565
20.2.1	Sicherer lokaler Zugang.....	565
20.2.2	Sicherer Fernzugang.....	569
20.2.3	Session-Sicherheit.....	570
20.3	Schutz der Anwenderdaten	571
20.3.1	Ablage auf Speichermedien.....	571
20.3.2	Verarbeitung im Speicher.....	572
20.3.3	Transit über ein Netzwerk.....	572
20.4	Konfigurationsmanagement.....	573
20.5	Protokollierung und Überwachung	574
20.5.1	Protokollierung und Auswertung.....	574
20.5.2	Überwachung im laufenden Betrieb	577

20.6	Selbstschutz des Betriebssystems	579
20.6.1	Härtung gegen spezifische Bedrohungen	579
20.6.2	Malwareschutz.....	583
20.6.3	Boot-Schutz	583
20.6.4	Verwaltung angeschlossener Geräte und Speichermedien	583
20.6.5	Reduktion der Angriffsfläche.....	584
20.6.6	Einschränkung des zulässigen Netzwerkverkehrs.....	585
	Zusammenfassung	586
	Literatur	586
21	Virtualisierung	587
	Einleitung	587
21.1	Vorteile von Virtualisierungslösungen	587
21.2	Nachteile von Virtualisierungslösungen	588
21.3	Servervirtualisierung.....	589
21.4	Plattformvirtualisierung (Container).....	590
21.5	Speichervirtualisierung (SAN)	591
21.6	Clientvirtualisierung (VDI)	592
21.7	Netzwerkvirtualisierung.....	593
21.8	Grundsätzliche Sicherheitsmaßnahmen	594
21.9	Abhängigkeiten und neue Angriffswege/Fehlkonfigurationen berücksichtigen	595
	Zusammenfassung	596
	Literatur	596
22	Sicherheit von mobilen Endgeräten	597
	Einleitung und Überblick	597
22.1	Herausforderungen.....	597
22.2	Generelle Security-Architekturen mobiler Systeme.....	599
22.3	Bindung an Hersteller/Store und Eingriffsmöglichkeiten des Benutzers	600
22.4	Bring your own Device	600
22.5	Mobile Device Management	602
	Zusammenfassung	604

23	Anwendungssicherheit	605
	Einleitung	605
	Definition gängiger Begriffe	605
	Das Sicherheitsdilemma	606
23.1	Secure Software Development Lifecycle	606
23.1.1	Phasen der Softwareentwicklung	606
23.1.2	Besonderheiten der »Supply Chain«	607
23.2	Schwachstellen in Anwendungen.....	608
23.3	Reifegradmodelle	609
23.4	Threat Modeling und Security Requirements.....	610
23.5	Secure Design	611
23.6	Kryptografie	613
23.7	Secure Coding	614
23.8	Verifikation und Audit.....	615
	Zusammenfassung	616
	Literatur	616
24	Technisches Löschen und Vernichten	621
	Einleitung	621
24.1	Anforderungen zum Löschen und Entsorgen	621
24.2	Realisierung durch ein Lösch- und Entsorgungskonzept.....	623
24.3	Speicherorte.....	624
24.4	Technische Löschmaßnahmen	627
24.4.1	Drei Schritte in Löschläufen	627
24.4.2	Anforderungen an Löschmechanismen.....	628
24.4.3	Grenzen des einfachen Löschs	629
24.4.4	Sicheres Löschen durch Überschreiben.....	629
24.4.5	Verschlüsselung und Löschen.....	630
24.4.6	Löschen auf USB-Sticks und anderen Flash-Medien.....	631
24.4.7	Vernichten und Entsorgen.....	634
24.4.8	Integration in den Arbeitsalltag	636
	Zusammenfassung	637
	Literatur	637

25	Datenschutzrechtliches Löschkonzept	641
	Einleitung	641
25.1	Vorgaben der DSGVO zum Löschen personenbezogener Daten	641
25.2	Vorgehensweise nach DIN 66398	643
25.3	Der Regelkatalog.....	645
25.3.1	Datenarten und Löschregeln	645
25.3.2	Verbindlichkeit des Regelkatalogs.....	649
25.3.3	Pflegeprozess für den Regelkatalog	649
25.4	Umsetzung	649
25.4.1	Löschmaßnahmen	649
25.4.2	Umsetzungsbereiche	650
25.4.3	Spezielle Aufgaben für die Umsetzung.....	651
25.4.4	Umsetzungsdefizite	652
25.5	Nutzen	652
	Zusammenfassung	654
	Literatur	654
26	Awareness	655
	Einleitung	655
26.1	»Risikofaktor« Mensch	656
26.1.1	Zur Wahrnehmung von Informationssicherheit	656
26.1.2	Randbedingungen und Konsequenzen.....	657
26.2	Durchführung von Awareness-Kampagnen	659
26.2.1	Kampagnen-Problematiken	659
26.2.2	Zielsetzung einer Awareness-Kampagne	661
26.3	Awareness in der Praxis.....	663
26.3.1	Erfolgsfaktoren	663
26.3.2	Beteiligte.....	664
26.3.3	Das Vier-Phasen-Konzept einer Awareness-Kampagne	665
26.3.4	Gamification	669
26.3.5	Erfolgsmessung	670
	Zusammenfassung	671
	Literatur	671

27	Malware und Content Security	673
	Einleitung und Historie.....	673
27.1	Historie	673
27.2	Technische Verbreitungswege und Funktionen.....	675
27.2.1	Ablauf einer Infektion	675
27.2.2	Verbreitungswege.....	675
27.2.3	Mobile Datenträger	680
27.3	Geschäftsmodelle und Auswirkungen.....	681
27.3.1	Motivation der Angreifer	681
27.3.2	Geschäftsmodelle	681
27.3.3	Auswirkungen von Schadsoftware	684
27.4	Gegenmaßnahmen.....	684
27.4.1	Abschottung von Systemen	685
27.4.2	Content-Analyse	686
27.4.3	Erfassung des Netzwerkverkehrs	689
27.4.4	Dekomposition der Inhalte und Header-Analyse.....	690
27.4.5	Klassifikation von Inhalten	691
27.4.6	Ergebnisgesteuerte Aktionen.....	692
27.4.7	Besonderheiten bei der Nutzung eines Content-Filters für Anti-Spam-Maßnahmen	693
27.4.8	Content-Filter und verschlüsselte Inhalte	695
27.4.9	Verhaltensanalyse.....	696
27.4.10	Mikrovirtualisierung	697
	Literatur	697
28	Intrusion Detection	699
	Einleitung.....	699
28.1	Einordnung und Definitionen.....	699
28.2	Architektur und Komponenten von Intrusion-Detection-Systemen	700
28.3	Grundproblem der Analyse – oder »der Schein trügt«	703
28.4	Typen von Intrusion-Detection-Systemen.....	704
28.4.1	Host-based Intrusion-Detection-Systeme	704
28.4.2	Network-based Intrusion-Detection-System	705
28.4.3	Hybride Intrusion-Detection-Systeme	705

28.5	Komponenten von Intrusion-Detection-Systemen.....	706
28.5.1	Hostsensoren	706
28.5.2	Netzsensoren	707
28.5.3	Datenbankkomponenten	707
28.5.4	Managementstation	708
28.5.5	Auswertungstation	708
28.6	Methoden der Angriffserkennung	708
28.6.1	Erkennen von Angriffsmustern	709
28.6.2	Anomalieerkennung	709
28.6.3	Korrelation von Ereignisdaten	710
28.7	Das Intrusion-Detection-Dilemma	710
28.8	Ausblick und Vorgaben für IDS	711
28.8.1	Anforderungen an die Sicherheitsadministration	712
28.8.2	Auswahl und Test eines IDS	713
	Zusammenfassung	714
	Literatur	714
29	Datensicherung	717
	Einleitung	717
29.1	Zwecke der Datensicherung	717
29.2	Strategien der Datensicherung	719
29.3	Technische Mechanismen	721
29.4	Backups von vertraulichen Daten	722
29.5	Backup-Medien	723
29.6	Datensicherung in der Cloud	724
29.7	Erfolgsfaktoren für Recovery	725
29.7.1	Physische Verfügbarkeit	725
29.7.2	Betriebliche Voraussetzungen für Recovery	726
29.7.3	Recovery-Fähigkeit überprüfen	726
29.8	Datensicherungskonzept	727
	Zusammenfassung	728
	Literatur	728

30	Incident-Management und Computer-Emergency-Response-Teams	729
	Einleitung	729
30.1	Ziel und Aufgaben des Incident-Managements	729
30.2	Der Aufbau des CERT	730
30.3	Regelmäßige Aufgaben des CERT	735
30.3.1	Überwachen der Informationsströme – Erkennen von Incidents.	735
30.3.2	Aufbau- und Pflegearbeiten	738
30.4	Der Incident-Prozess	739
30.4.1	Phase 1: Analysieren	739
30.4.2	Phase 2: Reagieren	744
30.4.3	Phase 3: Nachbereitung	746
	Zusammenfassung	747
	Literatur	747
	Übersicht über CERT-Organisationen	748
31	Business-Continuity-Management	751
	Einleitung	751
31.1	Business Continuity	752
31.1.1	Hohe Verfügbarkeit erreichen und schwere Störfälle beherrschen.	752
31.1.2	Business-Impact-Analyse	753
31.1.3	Verantwortung für Business Continuity	758
31.2	Business Continuity vorbereiten	758
31.2.1	Notfall-Teams und Krisenstab etablieren	759
31.2.2	Störfalleskalationswege aufbauen	760
31.2.3	Notfallhandbuch bereitstellen	762
31.2.4	Notfallvorsorge	764
31.2.5	Krisenkommunikation vorbereiten	766
31.2.6	BC-Training, BC-Awareness und BC-Kultur	766
31.3	BCM etablieren	767
31.3.1	Das BCM-Team	768
31.3.2	Initialisierung des Business-Continuity-Managements	768
31.3.3	BCM-Planungsphase	769
31.3.4	Umsetzungsphase	770
31.3.5	Überwachung	771
31.3.6	Weiterentwicklung	772

31.4	Standards für BCM.....	772
31.4.1	ISO 22301	773
31.4.2	ISO 22313	774
31.4.3	ISO/IEC 27031	775
31.4.4	BSI-Standard 100-4 Notfallmanagement.....	776
31.4.5	BCI Good Practice Guidelines	777
	Zusammenfassung	778
	Literatur	779
32	Cloud Security	781
	Einleitung	781
32.1	Cloud-Modelle und Cloud-Angebote.....	781
32.2	Gefahren der Cloud-Nutzung.....	784
32.3	Identitäts- und Berechtigungsmanagement.....	785
32.4	Verschlüsselung	786
32.5	Konfigurationsmanagement.....	786
32.6	Weitere Sicherheitsaspekte Cloud Security	787
	Zusammenfassung	789
	Literatur	789
	Anhang	791
	Übersicht zu Standards der Informationssicherheit	793
	Index	831
	Abkürzungen und Glossar	855