

Inhaltsübersicht

Vorwort.....	iv
Vorwort des TeleTrust Deutschland e. V.	v
1 Aufgaben und Ziele der Informationssicherheit	1
2 Betriebswirtschaftliche Aspekte der Informationssicherheit	15
3 Rechtliche Aspekte der Informationssicherheit.....	31
4 Hackermethoden	113
5 ISO 27001 und ISO 27002.....	127
6 IT-Grundschutz.....	145
7 Sicherheitskonzept.....	163
8 Physische Sicherheit	169
9 Netzwerksicherheit	183
10 Firewalls.....	243
11 Kryptografie.....	257
12 Vertrauensmodelle und PKI-Komponenten.....	299
13 Virtual Private Networks.....	327
14 Sicherheit in mobilen Netzen.....	351
15 Authentifizierung und Berechtigungsmanagement	393
16 Betriebssystemsicherheit.....	433
17 Windows-Sicherheit.....	465
18 Unix-Sicherheit	505
19 Sicherheit von mobilen Endgeräten	549
20 Web Security und Anwendungssicherheit	557
21 Löschen und Entsorgen	573
22 Awareness	591
23 Malware und Content Security.....	609
24 Intrusion Detection.....	635
25 Datensicherung	653
26 Incident-Management und Computer Emergency Response Teams	665
27 Business-Continuity-Management	687
Übersicht zu Standards der Informationssicherheit	717
Index.....	749
Abkürzungen und Glossar	781

Inhaltsverzeichnis

Vorwort	iv
<hr/>	
Vorwort des TeleTrust Deutschland e. V.	v
<hr/>	
1 Aufgaben und Ziele der Informationssicherheit	1
<hr/>	
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	5
1.1.5 Sicherheitskonzept erstellen	5
1.1.6 Sicherheitsmaßnahmen überprüfen	7
1.2 Generische Sicherheitsziele	8
1.2.1 Vertraulichkeit	9
1.2.2 Integrität	9
1.2.3 Verfügbarkeit	10
1.2.4 Authentizität	11
1.2.5 Sicherheitsziele und Sicherheitskonzept	12
2 Betriebswirtschaftliche Aspekte der Informationssicherheit	15
<hr/>	
2.1 Quantitative Modelle	16
2.1.1 Kosten von Risiken	17
2.1.2 Kosten von Sicherheitsvorfällen	18
2.1.3 Kosten von Sicherheitsmaßnahmen	19
2.1.4 Das ROSI-Modell	20
2.1.5 Grenzen des ROSI-Ansatzes	21
2.1.6 Alternative quantitative Modelle	22
2.2 Qualitative Betrachtungen	25
2.2.1 Grenzen betriebswirtschaftlicher Betrachtungen	25
2.2.2 Wirtschaftlichkeit von Investitionsentscheidungen	25
2.2.3 Risikomatrix	26
2.2.4 Pareto-Prinzip	27
2.2.5 Erfahrungswerte – Best Practice	27

3 Rechtliche Aspekte der Informationssicherheit **31**

3.1 Informationssicherheit und Recht	33
3.1.1 Risikomanagement als rechtliche Anforderung	34
3.1.2 Anforderungen aus dem Gesellschaftsrecht	36
3.1.3 Anforderungen aus dem Bankenrecht	40
3.1.4 Anforderungen aus dem Steuer- und Handelsrecht	44
3.1.5 Informationssicherheit für Kritische Infrastrukturen (IT-Sicherheitsgesetz)	46
3.2 Datenschutzrecht	51
3.2.1 Grundzüge des Datenschutzrechts	52
3.2.2 Grundlagen zur Informationssicherheit im Datenschutzrecht	62
3.3 Telekommunikationsrecht	67
3.3.1 Grundlagen zur Informationssicherheit im Telekommunikationsrecht	68
3.3.2 Anforderungen an Informationssicherheit im Telekommunikationsrecht	69
3.3.3 Durchsetzung von Informationssicherheit im Telekommunikationsrecht	70
3.4 Telemedienrecht	71
3.4.1 Grundlagen zur Informationssicherheit im Telemedienrecht	72
3.4.2 Anforderungen an Informationssicherheit im Telemedienrecht	73
3.4.3 Durchsetzung von Informationssicherheit im Telemedienrecht	74
3.5 Strafrecht	75
3.5.1 Grundlagen zur Informationssicherheit im Strafrecht	76
3.5.2 Anforderungen an Informationssicherheit im Strafrecht	79
3.5.3 Durchsetzung von Informationssicherheit im Strafrecht	79
3.5.4 Schutz der Informationsverarbeitung durch Strafrecht	80
3.6 Verträge und Vertragsrecht	82
3.6.1 Anforderungen an Informationssicherheit in Verträgen und im Vertragsrecht	83
3.6.2 Durchsetzung von Informationssicherheit in Verträgen und im Vertragsrecht	84
3.7 Arbeitsrecht	85
3.7.1 Arbeitsrecht als Gestaltungsmittel der Informationssicherheit	86
3.7.2 Regelungen im Arbeitsverhältnis	86
3.7.3 Regelungen durch Betriebsvereinbarung	89
3.8 Regulierte Infrastrukturen	90
3.8.1 eIDAS-Verordnung	91
3.8.2 Rolle und Anforderungen an Vertrauensdiensteanbieter	93
3.8.3 Arten von elektronischen Signaturen	95
3.8.4 Anforderungen an die Erstellung qualifizierter Zertifikate	97
3.8.5 Rechtsfolgen und Beweisrecht beim Einsatz Vertrauensdiensten	98
3.8.6 De-Mail im Lichte der eIDAS-VO und des Vertrauensdienstegesetzes	100
3.9 Rechtliche Grenzen für Sicherheitsmaßnahmen	102
3.9.1 Datenschutzrecht	103
3.9.2 Telekommunikationsrecht	106
3.9.3 Telemedienrecht	109
3.9.4 Betriebliche Mitbestimmung	109

4	Hackermethoden	113
4.1	Begriffsdefinition »Hacker«	113
4.2	Ursachen von Sicherheitsproblemen	113
4.2.1	SQL-Injection	114
4.2.2	Buffer Overflows	115
4.2.3	Motivation eines Angreifers	117
4.3	Vorgehensweise bei Penetrationstests	118
4.3.1	Informationsbeschaffung	118
4.3.2	Portscans	119
4.3.3	Automatische Überprüfungen	120
4.3.4	Manuelle Untersuchungen	121
4.3.5	Anwendung von Exploits	121
4.3.6	Social Engineering	122
4.4	Angriffswerkzeuge.....	122
4.4.1	Rootkits.....	124
4.4.2	Virus Construction Kits	124
4.4.3	Trojaner.....	124
5	ISO 27001 und ISO 27002	127
5.1	Entstehungsgeschichte	127
5.2	Die Familie der ISO 27000-Standards.....	129
5.3	ISO 27001	131
5.3.1	Vorgehensweise und Anwendungen.....	131
5.3.2	Inhaltliche Elemente der ISO 27001	132
5.3.3	Notwendige Dokumentation	135
5.3.4	Prüfungs- und Zertifizierungsprozess	137
5.4	ISO 27002	138
6	IT-Grundschutz	145
6.1	Historie.....	145
6.2	IT-Grundschutz – der Ansatz	146
6.3	IT-Grundschutz-Dokumente	147
6.3.1	BSI-Standard 200-1: Managementsysteme für Informationssicherheit	148
6.3.2	BSI-Standard 200-2: IT-Grundschutz-Vorgehensweise	150
6.3.3	BSI-Standard 200-3: Risikomanagement.....	157
6.3.4	BSI-Standard 100-4: Notfallmanagement	158
6.3.5	IT-Grundschutz-Kompodium	158
6.4	Tool-Unterstützung.....	159
6.5	ISO 27001-Zertifizierung auf Basis von IT-Grundschutz	159

7	Sicherheitskonzept	163
7.1	Ziele des Sicherheitskonzepts.....	163
7.2	Zentrale Aufgaben im Sicherheitskonzept	165
7.2.1	Berechtigte und Unberechtigte.....	165
7.2.2	Schwachstellen vermeiden.....	166
7.2.3	Identifikation von Unregelmäßigkeiten	167
7.2.4	Reaktionen auf Störfälle	167
8	Physische Sicherheit	169
8.1	Bedrohungen	169
8.2	Erhöhung der Gebäudesicherheit	170
8.2.1	Bewusste Standortwahl.....	170
8.2.2	Sichere bauliche Gestaltung.....	171
8.2.3	Schutzzonen	172
8.2.4	Rettungs- und Fluchtwege	174
8.3	Angemessene Überwachung	175
8.4	Monitoring und automatisierte Maßnahmensteuerung.....	176
8.5	Wirksamer Brandschutz.....	176
8.6	Stromversorgung	177
8.7	Physische Schutzmaßnahmen in externen Bereichen.....	178
8.7.1	Mobile Endgeräte	178
8.7.2	Häuslicher Arbeitsplatz	178
8.7.3	Datenträger	178
9	Netzwerksicherheit	183
9.1	Das OSI-Modell.....	183
9.1.1	Protokolle, Adressen und Ports.....	186
9.1.2	Bedrohungen	188
9.2	Das Internet Protocol.....	189
9.3	IPv4.....	191
9.3.1	Address Resolution Protocol – ARP.....	191
9.3.2	Bedrohungen gegen IPv4.....	193
9.4	IPv6.....	196
9.4.1	Unterschiede zwischen IPv6 und IPv4	196
9.4.2	Neighbor Discovery	199
9.4.3	Header-Erweiterungen.....	201
9.4.4	Fragmentierung.....	202
9.4.5	Privatsphäre.....	203
9.4.6	Netzwerk-Scans.....	205
9.4.7	Produkte und Implementierungen	206

9.5 Multiprotocol Label Switching – MPLS	207
9.6 Transportprotokolle.....	207
9.6.1 Sicherheitsmechanismen in Transportprotokollen.....	208
9.6.2 Übersicht über verschiedene Transportprotokolle	212
9.7 Netzwerkmanagementprotokolle.....	212
9.7.1 Konfigurationsprotokolle.....	213
9.7.2 Auskunftsdienste	216
9.7.3 Routing-Protokolle	220
9.7.4 Anmerkung zu verschiedenen Sicherheitsmechanismen der Protokolle	223
9.8 Sicherheitsmechanismen für Netzwerke.....	223
9.8.1 IEEE 802.1X.....	223
9.8.2 IPsec	226
9.8.3 SSL/TLS	227
9.8.4 Datagram Transport Layer Security – DTLS.....	229
9.8.5 Secure Shell – SSH	229
9.8.6 Überwachung des Netzwerkverkehrs.....	230
9.9 Netzarchitektur.....	231
9.9.1 Einteilung des Netzes in Zonen	231
9.9.2 Zugriffskontrolle auf Switchen	234
9.9.3 Virtuelle LANs	235
9.9.4 Network Address Translation.....	238

10 Firewalls 243

10.1 Grundlagen von Firewalls	243
10.2 Firewall-Typen	245
10.2.1 Paketfilter	246
10.2.2 Application Level Gateway.....	246
10.2.3 Stealth Gateway.....	247
10.2.4 Unified Threat Management (UTM)	248
10.3 Firewall-Architekturen.....	248
10.3.1 Einstufige Paketfilter-Architektur.....	248
10.3.2 Multi-Homed-Architektur	249
10.3.3 Demilitarisierte Zone	250
10.3.4 PAP-Firewall-Architekturen.....	252
10.4 Firewall-Konzepte	254
10.4.1 Anforderungsanalyse für den Firewall-Einsatz	254
10.4.2 Betriebliche Anforderungen für die Firewall-Konzeption	255
10.5 Grenzen von Firewalls.....	255

11 Kryptografie 257

11.1	Vorgehensweise.....	258
11.2	Begriffsklärung.....	259
11.3	Angriffs- und Sicherheitsziele	260
11.3.1	Lesen von Daten – Vertraulichkeit	260
11.3.2	Ändern von Daten – Integrität	261
11.3.3	Wiedereinspielen von Daten – Frische	261
11.3.4	Vortäuschen einer Identität – Urheber-Authentizität.....	262
11.3.5	Abstreiten der Verantwortung – Nicht-Abstreitbarkeit.....	262
11.3.6	Weitere Angriffs- und Sicherheitsziele.....	262
11.4	Grundsätzliche Angriffsszenarien	263
11.5	Sichere Kanäle.....	265
11.5.1	Verschlüsselung.....	265
11.5.2	Chiffrierverfahren.....	266
11.5.3	Betriebsmodi	272
11.5.4	Integrität	276
11.5.5	Authentisierte Verschlüsselung	280
11.5.6	Weitere Anwendungen	282
11.6	Herausforderung Schlüsselverteilung	282
11.6.1	Der direkte Weg.....	282
11.6.2	Indirekt über vertrauenswürdige Dritte.....	284
11.7	Asymmetrische Verfahren zur Schlüsselverteilung	286
11.7.1	Grundprinzipien asymmetrischer Verfahren.....	286
11.7.2	Schlüsseltransport.....	286
11.7.3	Schlüsselaustausch.....	288
11.8	Digitale Signaturen	290
11.8.1	Grundprinzipien digitaler Signaturen.....	290
11.8.2	Digitale Signaturen für die Nicht-Abstreitbarkeit	292
11.8.3	Digitale Signaturen für Zertifikate	292
11.9	Praktischer Einsatz.....	293
11.9.1	Schlüssellängen	293
11.9.2	Proprietäre Verfahren.....	294
11.9.3	Proprietäre Implementierungen	295
11.9.4	Erzeugung von Zufallszahlen	295

12 Vertrauensmodelle und PKI-Komponenten 299

12.1	Vertrauensmodelle	300
12.1.1	Web of Trust.....	300
12.1.2	Zentrales Modell der Public Key Infrastruktur.....	302
12.2	Public Key Infrastruktur.....	303
12.2.1	Zertifikate und CRLs	303
12.2.2	Zertifizierungshierarchien.....	306
12.2.3	Verifikation einer digitalen Signatur	306
12.2.4	Komponenten und Prozesse einer PKI	308
12.2.5	Policies für Public Key Infrastrukturen.....	316

12.3 Standards im Bereich PKI	317
12.3.1 X.509 Standard	317
12.3.2 PKIX-Standards.....	317
12.3.3 PKCS-Standards.....	318
12.3.4 Common PKI Spezifikationen	319
12.4 Verknüpfung von Public Key Infrastrukturen.....	320
12.5 Langzeitarchivierung	323

13 Virtual Private Networks **327**

13.1 VPN-Szenarien	328
13.1.1 Site-to-Site-VPN.....	328
13.1.2 End-to-Site-VPN.....	329
13.1.3 End-to-End-VPN.....	329
13.1.4 Protokollebenen von VPN und VPN-Tunnel.....	330
13.2 Technische Realisierung von VPN	331
13.2.1 PPP, L2F und PPTP	331
13.2.2 Layer 2 Tunneling Protocol – L2TP.....	333
13.2.3 IP Security – IPsec	337
13.2.4 OpenVPN.....	346
13.3 Spezielle Risiken von VPN	348

14 Sicherheit in mobilen Netzen **351**

14.1 Bedrohungen in mobilen Netzen.....	351
14.2 Wireless LAN.....	353
14.2.1 Entwicklung und Standardisierung.....	353
14.2.2 Netzarchitektur und Netzkomponenten	354
14.2.3 Sicherheitsverfahren.....	355
14.2.4 Empfohlene Sicherheitsmaßnahmen.....	360
14.3 Bluetooth.....	361
14.3.1 Entwicklung und Standardisierung.....	361
14.3.2 Netzarchitektur und -komponenten	362
14.3.3 Sicherheitsverfahren in Bluetooth.....	364
14.3.4 Bluetooth-Sicherheitsmechanismen im Detail	370
14.3.5 Bewertung der Sicherheitsmaßnahmen.....	374
14.4 Mobilfunk.....	376
14.4.1 GSM	376
14.4.2 GPRS	385
14.4.3 UMTS.....	386
14.4.4 LTE.....	390

15 Authentifizierung und Berechtigungsmanagement **393**

15.1 Benutzer.....	394
15.2 Identität.....	394
15.3 Identifizierung.....	395
15.4 Authentifizierung.....	395
15.4.1 Authentifizierung durch Wissen.....	396
15.4.2 Authentifizierung durch Besitz.....	404
15.4.3 Authentifizierung durch Biometrie.....	406
15.4.4 Authentifizierung in verteilten Systemen.....	407
15.5 Autorisierung und Zugriffskontrolle.....	412
15.5.1 Zugriffsrechtematrix.....	413
15.5.2 Zugriffskontrolllisten.....	414
15.5.3 Capabilities.....	414
15.5.4 Rollenbasierte Zugriffskontrolle.....	415
15.5.5 Nachteile von Zugriffskontrollstrategien.....	416
15.6 Identitäts- und Berechtigungsmanagement.....	416
15.7 Single Sign-On.....	418
15.7.1 Unternehmensweites Single Sign-On.....	418
15.7.2 SSO für Web-Services.....	420
15.7.3 OpenID.....	424
15.7.4 OAuth 2.0.....	425
15.7.5 OpenID-Connect.....	425
15.7.6 SAML.....	426
15.7.7 Mozilla Persona.....	427
15.7.8 Sicherheit von SAML, OpenID, OAuth und Mozilla Persona.....	429

16 Betriebssystemsicherheit **433**

16.1 Identität und Autorisierung.....	434
16.1.1 Benutzer, Benutzergruppen und Rollen.....	435
16.1.2 Ressourcen.....	436
16.1.3 Zugriffsrechte.....	436
16.1.4 Erweiterung von Rechten – privilegierte Aktionen.....	437
16.2 Systemzugang und Authentisierung.....	438
16.2.1 Sicherer lokaler Zugang.....	438
16.2.2 Sicherer Fernzugang.....	438
16.2.3 Session-Sicherheit.....	445
16.3 Schutz der Anwenderdaten.....	446
16.3.1 Ablage auf Speichermedien.....	446
16.3.2 Verarbeitung im Speicher.....	448
16.3.3 Transit über ein Netzwerk.....	449

16.4 Konfigurationsmanagement	449
16.5 Protokollierung und Überwachung.....	451
16.5.1 Protokollierung und Auswertung.....	451
16.5.2 Überwachung im laufenden Betrieb	453
16.6 Selbstschutz und Härtung des Betriebssystems	454
16.6.1 Härtung gegen spezifische Bedrohungen	454
16.6.2 Malwareschutz	457
16.6.3 Boot-Schutz.....	459
16.6.4 Verwaltung angeschlossener Geräte und Speichermedien	460
16.6.5 Reduktion der Angriffsfläche	461
16.6.6 Einschränkung des zulässigen Netzwerkverkehrs	462
17 Windows-Sicherheit	465
17.1 Identifizierung und Autorisierung	466
17.1.1 Benutzer, Benutzergruppen und Rollen	466
17.1.2 Ressourcen.....	470
17.1.3 Zugriffsrechte.....	473
17.1.4 Erweiterung von Rechten – privilegierte Aktionen	477
17.2 Systemzugang und Authentisierung	479
17.2.1 Sicherer lokaler Zugang	479
17.2.2 Sicherer Fernzugang	480
17.2.3 Session-Sicherheit	485
17.3 Schutz der Anwenderdaten	486
17.3.1 Ablage auf Speichermedien	486
17.3.2 Verarbeitung im Speicher	486
17.3.3 Transit über ein Netzwerk	487
17.4 Konfigurationsmanagement	487
17.4.1 Die Registry.....	487
17.4.2 Active Directory Domain Services.....	488
17.4.3 Gruppenrichtlinien.....	489
17.4.4 Management-Werkzeuge	489
17.5 Protokollierung und Überwachung.....	490
17.5.1 Protokollierung und Auswertung.....	490
17.5.2 Überwachung im laufenden Betrieb	496
17.6 Selbstschutz und Härtung des Betriebssystems	497
17.6.1 Härtung gegen spezifische Bedrohungen	497
17.6.2 Malwareschutz	498
17.6.3 Bootschutz.....	500
17.6.4 Verwaltung angeschlossener Geräte und Speichermedien	500
17.6.5 Reduktion der Angriffsfläche	501
17.6.6 Einschränkung des zulässigen Netzwerkverkehrs	501

18 Unix-Sicherheit	505
18.1 Identität und Autorisierung	506
18.1.1 Benutzer, Benutzergruppen und Rollen	506
18.1.2 Ressourcen.....	511
18.1.3 Zugriffsrechte.....	517
18.1.4 Erweiterung von Rechten – privilegierte Aktionen	524
18.2 Systemzugang und Authentisierung	526
18.2.1 Sicherer lokaler Zugang	526
18.2.2 Sicherer Fernzugang	530
18.2.3 Session-Sicherheit	532
18.3 Schutz der Anwenderdaten	533
18.3.1 Ablage auf Speichermedien	533
18.3.2 Verarbeitung im Speicher	534
18.3.3 Transit über ein Netzwerk	534
18.4 Konfigurationsmanagement	535
18.5 Protokollierung und Überwachung.....	535
18.5.1 Protokollierung und Auswertung.....	535
18.5.2 Überwachung im laufenden Betrieb.....	538
18.6 Selbstschutz des Betriebssystems	540
18.6.1 Härtung gegen spezifische Bedrohungen	540
18.6.2 Malwareschutz	545
18.6.3 Boot-Schutz.....	545
18.6.4 Verwaltung angeschlossener Geräte und Speichermedien	546
18.6.5 Reduktion der Angriffsfläche	546
18.6.6 Einschränkung des zulässigen Netzwerkverkehrs	547
19 Sicherheit von mobilen Endgeräten	549
19.1 Problemaufriss.....	549
19.2 Generelle Security-Architekturen mobiler Systeme.....	551
19.3 Bindung an Hersteller/Store und Eingriffsmöglichkeiten des Benutzers.....	552
19.4 Bring your own Device.....	553
19.5 Mobile Device Management.....	554
20 Web Security und Anwendungssicherheit	557
20.1 Einführung in Webanwendungen	557
20.2 Ausgewählte Angriffe	563
20.3 Sicherung von Web-Anwendungen.....	566
20.3.1 Konkrete Abwehrmaßnahmen	567
20.3.2 Entwurf und Entwicklung sicherer Web-Anwendungen	568
20.3.3 Testen der Sicherheit von Web-Anwendungen	569

21 Löschen und Entsorgen	573
21.1 Anforderungen zum Löschen und Entsorgen.....	573
21.2 Lösch- und Entsorgungskonzept.....	576
21.3 Speicherorte.....	577
21.4 Technische Löschmaßnahmen.....	580
21.4.1 Einfaches Löschen.....	581
21.4.2 Sicheres Löschen.....	581
21.4.3 Verschlüsselung und Löschen.....	582
21.4.4 Löschen auf USB-Sticks und anderen Flash-Medien.....	583
21.4.5 Vernichten und Entsorgen.....	584
22 Awareness	591
22.1 »Risikofaktor« Mensch.....	591
22.1.1 Zur Wahrnehmung von IT-Sicherheit.....	592
22.1.2 Randbedingungen und Konsequenzen.....	593
22.2 Durchführung von Awareness-Kampagnen.....	594
22.2.1 Kampagnen-Problematiken.....	594
22.2.2 Zielsetzung einer Awareness-Kampagne.....	596
22.3 Awareness in der Praxis.....	598
22.3.1 Erfolgsfaktoren.....	598
22.3.2 Beteiligte.....	600
22.3.3 Das Vier-Phasen-Konzept einer Awareness-Kampagne.....	600
22.3.4 Erfolgsmessung.....	605
23 Malware und Content Security	609
23.1 Historie.....	609
23.2 Technische Verbreitungswege und Funktionen.....	611
23.2.1 Ablauf einer Infektion.....	611
23.2.2 Verbreitungswege.....	611
23.2.3 Mobile Datenträger.....	616
23.3 Geschäftsmodelle und Auswirkungen.....	616
23.3.1 Motivation der Angreifer.....	616
23.3.2 Geschäftsmodelle.....	617
23.3.3 Auswirkungen von Schadsoftware.....	620
23.4 Gegenmaßnahmen.....	620
23.4.1 Abschottung von Systemen.....	621
23.4.2 Content-Analyse.....	622
23.4.3 Erfassung des Netzwerkverkehrs.....	624
23.4.4 Dekomposition der Inhalte und Header-Analyse.....	626
23.4.5 Klassifikation von Inhalten.....	627
23.4.6 Aktionen.....	628
23.4.7 Besonderheiten bei der Nutzung eines Content-Filters für Anti-Spam-Maßnahmen.....	629
23.4.8 Content-Filter und verschlüsselte Inhalte.....	631
23.4.9 Verhaltensanalyse.....	631
23.4.10 Mikrovirtualisierung.....	632

24 Intrusion Detection **635**

24.1 Einordnung und Definitionen	635
24.2 Architektur und Komponenten von Intrusion-Detection-Systemen.....	636
24.3 Grundproblem der Analyse – oder »der Schein trügt«	639
24.4 Typen von Intrusion-Detection-Systemen	640
24.4.1 <i>Host-based Intrusion-Detection-Systeme</i>	640
24.4.2 <i>Network-based Intrusion-Detection-System</i>	641
24.4.3 <i>Hybride Intrusion-Detection-Systeme</i>	641
24.5 Komponenten von Intrusion-Detection-Systemen	642
24.5.1 <i>Hostsensoren</i>	642
24.5.2 <i>Netzsensoren</i>	643
24.5.3 <i>Datenbankkomponenten</i>	643
24.5.4 <i>Managementstation</i>	644
24.5.5 <i>Auswertungsstation</i>	644
24.6 Methoden der Angriffserkennung	644
24.6.1 <i>Erkennen von Angriffsmustern</i>	645
24.6.2 <i>Anomalieerkennung</i>	645
24.6.3 <i>Korrelation von Ereignisdaten</i>	646
24.7 Das Intrusion-Detection-Dilemma	646
24.8 Ausblick und Vorgaben für IDS	647
24.8.1 <i>Anforderungen an die Sicherheitsadministration</i>	648
24.8.2 <i>Auswahl und Test eines IDS</i>	649

25 Datensicherung **653**

25.1 Zwecke der Datensicherung	653
25.2 Strategien der Datensicherung	655
25.3 Technische Mechanismen	657
25.4 Backups von vertraulichen Daten	658
25.5 Backup-Medien	659
25.6 Erfolgsfaktoren für Recovery.....	660
25.6.1 <i>Physische Verfügbarkeit</i>	660
25.6.2 <i>Betriebliche Voraussetzungen für Recovery</i>	661
25.6.3 <i>Recovery-Fähigkeit überprüfen</i>	661
25.7 Datensicherungskonzept.....	662

26 Incident-Management und Computer Emergency Response Teams	665
26.1 Ziel und Aufgaben des Incident-Management.....	665
26.2 Der Aufbau des CERT	666
26.3 Regelmäßige Aufgaben des CERT.....	671
26.3.1 Überwachen der Informationsströme – Erkennen von Incidents	671
26.3.2 Aufbau- und Pflegearbeiten.....	673
26.4 Der Incident-Prozess.....	674
26.4.1 Phase 1: Analysieren.....	675
26.4.2 Phase 2: Reagieren	680
26.4.3 Phase 3: Nachbereitung	681
27 Business-Continuity-Management	687
27.1 Business Continuity	687
27.1.1 Hohe Verfügbarkeit erreichen und schwere Störfälle beherrschen	687
27.1.2 Business-Impact-Analyse	688
27.1.3 Verantwortung für Business Continuity.....	694
27.2 Business Continuity vorbereiten	694
27.2.1 Notfall-Teams und Krisenstab etablieren	695
27.2.2 Störfall-Eskalationswege aufbauen	696
27.2.3 Notfallhandbuch bereitstellen.....	698
27.2.4 Notfallvorsorge	700
27.2.5 Krisenkommunikation vorbereiten	702
27.2.6 BC-Training, BC-Awareness, und BC-Kultur	702
27.3 BCM etablieren.....	704
27.3.1 Das BCM-Team	704
27.3.2 Initialisierung des Business-Continuity-Management.....	704
27.3.3 BCM-Planungsphase.....	705
27.3.4 Umsetzungsphase	706
27.3.5 Überwachung	707
27.3.6 Weiterentwicklung	708
27.4 Standards für BCM.....	709
27.4.1 ISO 22301.....	709
27.4.2 ISO 22313.....	711
27.4.3 ISO/IEC 27031.....	711
27.4.4 BSI-Standard 100-4 Notfallmanagement.....	712
27.4.5 BCI Good Practice Guidelines	713
Übersicht zu Standards der Informationssicherheit	717
Index	749
Abkürzungen und Glossar	781