Inhaltsverzeichnis

Vorwort IV

Vorwort des TeleTrusT Deutschland e.V. V

Inhaltsübersicht VI

Inhaltsverzeichnis VII

1 Aufgaben und Ziele der Informationssicherheit 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 Integrität 8
1.2.2 Integrität 9
1.2.3 Verfügbarkeit 9
1.2.4 Authentizität 10
1.2.5 Sicherheitsziele und Sicherheitskonzept 11

2 Betriebswirtschaftliche Aspekte der Informationssicherheit 15

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 19
2.1.5 Grenzen des ROSI-Ansatzes 21
2.1.6 Alternative quantitative Modelle 22

2.2 Qualitative Betrachtungen 24
2.2.1 Grenzen betriebswirtschaftlicher Betrachtungen 24
2.2.2 Wirtschaftlichkeit von Investitionsentscheidungen 24
2.2.3 Risikomatrix 25
2.2.4 Pareto-Prinzip 25
2.2.5 Erfahrungswerte – Best Practice 26

3 Rechtliche Aspekte der Informationssicherheit 29

3.1 Informationssicherheit und Recht 30

3.2 Rechtsbereiche mit Sicherheitsanforderungen 31
3.2.1 Gesellschaftsrecht 31

3.2.2 Bankenrecht ... 35
3.2.3 Steuer- und Handelsrecht ... 38
3.2.4 Datenschutzrecht ... 39
3.2.5 Telekommunikationsrecht ... 50
3.2.6 Telemedienrecht ... 53
3.2.7 Strafrecht ... 56
3.2.8 Verträge und Vertragsrecht ... 62
3.3 Arbeitsrecht ... 64
3.3.1 Regelungen im Arbeitsverhältnis ... 66
3.3.2 Regelungen durch Betriebsvereinbarung ... 68
3.4 Regulierte Infrastrukturen ... 69
3.4.1 Signaturrecht ... 70
3.4.2 De-Mail ... 74
3.5 Rechtliche Grenzen für Sicherheitsmaßnahmen ... 76
3.5.1 Datenschutzrecht ... 76
3.5.2 Telekommunikationsrecht ... 80
3.5.3 Telemedienrecht ... 82
3.5.4 Betriebliche Mitbestimmung ... 82

4 Hackermethoden 87

4.1 Begriffsdefinition „Hacker“ ... 87
4.2 Ursachen von Sicherheitsproblemen ... 87
4.2.1 SQL-Injection ... 88
4.2.2 Buffer Overflows ... 89
4.2.3 Motivation eines Angreifers ... 91
4.3 Vorgehensweise bei Penetrationstests ... 91
4.3.1 Informationsbeschaffung ... 92
4.3.2 Portscans ... 92
4.3.3 Automatische Überprüfungen ... 94
4.3.4 Manuelle Untersuchungen ... 94
4.3.5 Anwendung von Exploits ... 95
4.3.6 Social Engineering ... 95
4.4 Angriffswerkzeuge ... 95
4.4.1 Rootkits ... 97
4.4.2 Virus Construction Kits ... 97
4.4.3 Trojaner ... 98

5 ISO 27001 und ISO 27002 103

5.1 Entstehungsgeschichte ... 103
5.2 Die Familie der ISO 27000-Standards ... 105
5.3 ISO 27001 ... 106
5.3.1 Vorgehensweise und Anwendungen ... 107
5.3.2 Inhaltliche Elemente der ISO 27001 ... 108
5.3.3 Notwendige Dokumentation ... 110
5.3.4 Prüfungs- und Zertifizierungsprozess ... 112

5.4 ISO 27002 113

6 IT-Grundschutz 119

6.1 Historie 119
6.2 IT-Grundschutz Ansatz 120
6.3 IT-Grundschutz Dokumente 121
6.3.1 BSI-Standard 100-1: Managementsysteme für Informationssicherheit 122
6.3.2 BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise 124
6.3.3 BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz 130
6.3.4 BSI-Standard 100-4: Notfallmanagement 131
6.3.5 IT-Grundschutz-Kataloge 131
6.4 Tool-Unterstützung 132
6.5 ISO 27001-Zertifizierung auf Basis von IT-Grundschutz 132

7 Sicherheitskonzept 135

7.1 Ziele des Sicherheitskonzepts 135
7.2 Zentrale Aufgaben im Sicherheitskonzept 137
7.2.1 Berechtigte und Unberechtigte 137
7.2.2 Schwachstellen vermeiden 138
7.2.3 Identifikation von Unregelmäßigkeiten 138
7.2.4 Reaktionen auf Störfälle 139

8 Physische Sicherheit 141

8.1 Bedrohungen 141
8.2 Erhöhung der Gebäudesicherheit 142
8.2.1 Bewusste Standortwahl 142
8.2.2 Sichere bauliche Gestaltung 143
8.2.3 Schutzzonen 143
8.2.4 Rettungs- und Fluchtwege 146
8.3 Angemessene Überwachung 146
8.4 Monitoring und automatisierte Maßnahmensteuerung 147
8.5 Wirksamer Brandschutz 147
8.6 Stromversorgung 148
8.7 Physische Schutzmaßnahmen in externen Bereichen 148
8.7.1 Mobile Endgeräte 149
8.7.2 Häuslicher Arbeitsplatz 149
8.7.3 Datenträger 149

9 Netzwerksicherheit 153

9.1 Das OSI-Modell 153
9.1.1 Protokolle, Adressen und Ports 156

9.1.2 Bedrohungen ... *157*

9.2 Das Internet Protocol ... 158

9.3 IPv4 ... 160

9.3.1 Address Resolution Protocol – ARP ... *160*

9.3.2 Bedrohungen gegen IPv4 ... *161*

9.4 IPv6 ... 164

9.4.1 Unterschiede zwischen IPv6 und IPv4 ... *164*

9.4.2 Neighbor Discovery ... *167*

9.4.3 Header-Erweiterungen ... *168*

9.4.4 Fragmentierung ... *169*

9.4.5 Privatsphäre ... *170*

9.4.6 Netzwerk-Scans ... *171*

9.4.7 Produkte und Implementierungen ... *172*

9.5 Multiprotocol Label Switching – MPLS ... 173

9.6 Transportprotokolle ... 173

9.6.1 Sicherheitsmechanismen in Transportprotokollen ... *174*

9.6.2 Übersicht über verschiedene Transportprotokolle ... *177*

9.7 Netzwerkmanagementprotokolle ... 178

9.7.1 Konfigurationsprotokolle ... *178*

9.7.2 Auskunftsdienste ... *181*

9.7.3 Routing-Protokolle ... *184*

9.7.4 Anmerkung zu verschiedenen Sicherheitsmechanismen der Protokolle ... *186*

9.8 Sicherheitsmechanismen für Netzwerke ... 187

9.8.1 IEEE 802.1X ... *187*

9.8.2 IPsec ... *189*

9.8.3 SSL/TLS ... *190*

9.8.4 Datagram Transport Layer Security – DTLS ... *192*

9.8.5 Secure Shell – SSH ... *192*

9.8.6 Überwachung des Netzwerkverkehrs ... *193*

9.9 Architektur ... 194

9.9.1 Einteilung des Netzes in Zonen ... *194*

9.9.2 Zugriffskontrolle auf Switchen ... *196*

9.9.3 Virtuelle LANs ... *197*

9.9.4 Network Address Translation ... *199*

10 Firewalls 203

10.1 Grundlagen von Firewalls ... 203

10.2 Firewall-Typen ... 205

10.2.1 Paketfilter ... *205*

10.2.2 Application Level Gateway ... *206*

10.2.3 Stealth Gateway ... *207*

10.3 Firewall-Architekturen ... 207

10.3.1 Einstufige Paketfilter-Architektur ... *207*

10.3.2 Multi-Homed-Architektur ... *208*

10.3.3 Demilitarisierte Zone ... *209*

10.3.4 PAP-Firewall-Architekturen ... *211*

10.4 Firewall-Konzepte 212
10.4.1 Anforderungsanalyse für den Firewall-Einsatz 212
10.4.2 Betriebliche Anforderungen für die Firewall-Konzeption 213
10.5 Grenzen von Firewalls 214

11 Kryptografie 215

11.1 Vorgehensweise 216
11.2 Begriffsklärung 217
11.3 Angriffs- und Sicherheitsziele 218
11.3.1 Lesen von Daten – Vertraulichkeit 218
11.3.2 Ändern von Daten – Integrität 219
11.3.3 Wiedereinspielen von Daten – Frische von Daten 219
11.3.4 Vortäuschen einer Identität – Urheber-Authentizität 219
11.3.5 Abstreiten der Verantwortung – Nicht-Abstreitbarkeit 219
11.3.6 Weitere Angriffs- und Sicherheitsziele 221
11.4 Grundsätzliche Angriffsszenarien 221
11.5 Sichere Kanäle 223
11.5.1 Verschlüsselung 223
11.5.2 Chiffrierverfahren 224
11.5.3 Betriebsmodi 228
11.5.4 Integrität 232
11.5.5 Authentisierte Verschlüsselung 236
11.5.6 Weitere Anwendungen 237
11.6 Herausforderungen der Schlüsselverteilung 238
11.6.1 Der direkte Weg 238
11.6.2 Der indirekte Weg über vertrauenswürdige Dritte 240
11.7 Asymmetrische Verfahren zur Schlüsselverteilung 241
11.7.1 Grundprinzipien asymmetrischer Verfahren 242
11.7.2 Schlüsseltransport 242
11.7.3 Schlüsselaustausch 244
11.8 Digitale Signaturen 246
11.8.1 Grundprinzipien digitaler Signaturen 246
11.8.2 Digitale Signaturen für die Nicht-Abstreitbarkeit 248
11.8.3 Digitale Signaturen für Zertifikate 249
11.9 Praktischer Einsatz 250
11.9.1 Schlüssellängen 250
11.9.2 Proprietäre Verfahren 251
11.9.3 Proprietäre Implementierungen 252
11.9.4 Erzeugung von Zufallszahlen 252

12 Vertrauensmodelle und PKI-Komponenten 255

12.1 Vertrauensmodelle 256
12.1.1 Web of Trust 256
12.1.2 Zentrales Modell der Public Key Infrastruktur 257

12.2 Public Key Infrastruktur 258
12.2.1 Zertifikate und CRLs 258
12.2.2 Zertifizierungshierarchien 260
12.2.3 Verifikation einer digitalen Signatur 261
12.2.4 Komponenten und Prozesse einer PKI 263
12.2.5 Policies für Public Key Infrastrukturen 269
12.3 Standards im Bereich PKI 269
12.3.1 X.509 Standard 270
12.3.2 PKIX-Standards 270
12.3.3 PKCS-Standards 270
12.3.4 Common PKI Spezifikationen 271
12.4 Verknüpfung von Public Key Infrastrukturen 272
12.5 Langzeitarchivierung 274

13 Virtual Private Networks 279

13.1 VPN-Szenarien 280
13.1.1 Site-to-Site-VPN 280
13.1.2 End-to-Site-VPN 281
13.1.3 End-to-End-VPN 281
13.1.4 Protokollebenen von VPNs und VPN-Tunnel 282
13.2 Technische Realisierung von VPN 283
13.2.1 PPP, L2F und PPTP 283
13.2.2 Layer 2 Tunneling Protocol – L2TP 284
13.2.3 IP Security – IPsec 288
13.2.4 OpenVPN 296
13.3 Spezielle Risiken von VPN 298

14 Authentifizierung und Berechtigungsmanagement 301

14.1 Benutzer 301
14.2 Identität 302
14.3 Identifizierung 302
14.4 Authentifizierung 303
14.4.1 Authentifizierung durch Wissen 303
14.4.2 Authentifizierung durch Besitz 310
14.4.3 Authentifizierung durch Biometrie 312
14.4.4 Authentifizierung in verteilten Systemen 313
14.5 Autorisierung und Zugriffskontrolle 317
14.5.1 Zugriffsrechtematrix 318
14.5.2 Zugriffskontrolllisten 318
14.5.3 Capabilities 319
14.5.4 Rollenbasierte Zugriffskontrolle 319
14.5.5 Nachteile von Zugriffskontrollstrategien 320
14.6 Identitäts- und Berechtigungsmanagement 321
14.7 Single Sign-On 322

14.7.1 Unternehmensweites Single Sign-On ... 322
14.7.2 SSO für Web-Services ... 323
14.7.3 OpenID ... 327
14.7.4 OAuth 2.0 ... 328
14.7.5 OpenID-Connect ... 328
14.7.6 SAML ... 329
14.7.7 Mozilla Persona ... 330
14.7.8 Sicherheit von SAML, OpenID, OAuth und Mozilla Persona ... 332

15 Sicherheit in mobilen Netzen 335

15.1 Bedrohungen in mobilen Netzen ... 335
15.2 Wireless LAN ... 337
15.2.1 Entwicklung und Standardisierung ... 337
15.2.2 Netzarchitektur und Netzkomponenten ... 338
15.2.3 Sicherheitsverfahren ... 339
15.2.4 Empfohlene Sicherheitsmaßnahmen ... 342
15.3 Bluetooth ... 344
15.3.1 Entwicklung und Standardisierung ... 344
15.3.2 Netzarchitektur und -komponenten ... 344
15.3.3 Sicherheitsverfahren in Bluetooth ... 345
15.3.4 Bluetooth-Sicherheitsmechanismen im Detail ... 351
15.3.5 Bewertung der Sicherheitsmaßnahmen ... 355
15.4 Mobilfunk ... 356
15.4.1 GSM ... 356
15.4.2 GPRS ... 364
15.4.3 UMTS ... 365
15.5 Mobile Anwendungen und Endgeräte ... 368
15.5.1 USB-Sticks ... 368
15.5.2 Anwendungsdaten und Zugriffsschutz ... 369
15.5.3 Smartphone Betriebssysteme und Sicherheitsmechanismen ... 370

16 Betriebssystemsicherheit 375

16.1 Identität und Autorisierung ... 376
16.1.1 Benutzer, Benutzergruppen und Rollen ... 376
16.1.2 Ressourcen ... 377
16.1.3 Zugriffsrechte ... 378
16.1.4 Erweiterung von Rechten – privilegierte Aktionen ... 378
16.2 Systemzugang und Authentisierung ... 379
16.2.1 Sicherer lokaler Zugang ... 379
16.2.2 Sicherer Fernzugang ... 380
16.2.3 Session-Sicherheit ... 385
16.3 Schutz der Anwenderdaten ... 386
16.3.1 Ablage auf Speichermedien ... 386
16.3.2 Verarbeitung im Speicher ... 388
16.3.3 Transit über ein Netzwerk ... 389
16.4 Konfigurationsmanagement ... 389

16.5 Protokollierung und Überwachung 390
16.5.1 Protokollierung und Auswertung 390
16.5.2 Überwachung im laufenden Betrieb 392
16.6 Selbstschutz und Härtung des Betriebssystems 393
16.6.1 Härtung gegen spezifische Bedrohungen 393
16.6.2 Malwareschutz 396
16.6.3 Boot-Schutz 397
16.6.4 Verwaltung angeschlossener Geräte und Speichermedien 398
16.6.5 Reduktion der Angriffsoberfläche 399
16.6.6 Einschränkung des zulässigen Netzwerkverkehrs 400

17 Windows-Sicherheit 403

17.1 Identifizierung und Autorisierung 404
17.1.1 Benutzer, Benutzergruppen und Rollen 404
17.1.2 Ressourcen 407
17.1.3 Zugriffsrechte 410
17.1.4 Erweiterung von Rechten – privilegierte Aktionen 413
17.2 Systemzugang und Authentisierung 416
17.2.1 Sicherer lokaler Zugang 416
17.2.2 Sicherer Fernzugang 417
17.2.3 Session-Sicherheit 422
17.3 Schutz der Anwenderdaten 422
17.3.1 Ablage auf Speichermedien 422
17.3.2 Verarbeitung im Speicher 423
17.3.3 Transit über ein Netzwerk 423
17.4 Konfigurationsmanagement 424
17.4.1 Die Registry 424
17.4.2 Active Directory Domain Services 424
17.4.3 Gruppenrichtlinien 425
17.4.4 Management-Werkzeuge 425
17.5 Protokollierung und Überwachung 426
17.5.1 Protokollierung und Auswertung 426
17.5.2 Überwachung im laufenden Betrieb 431
17.6 Selbstschutz und Härtung des Betriebssystems 432
17.6.1 Härtung gegen spezifische Bedrohungen 432
17.6.2 Malwareschutz 433
17.6.3 Bootschutz 435
17.6.4 Verwaltung angeschlossener Geräte und Speichermedien 435
17.6.5 Reduktion der Angriffsoberfläche 435
17.6.6 Einschränkung des zulässigen Netzwerkverkehrs 436

18 Unix-Sicherheit 439

18.1 Identität und Autorisierung 440
18.1.1 Benutzer, Benutzergruppen und Rollen 440
18.1.2 Ressourcen 444
18.1.3 Zugriffsrechte 449

18.1.4 Erweiterung von Rechten – privilegierte Aktionen ... 456

18.2 Systemzugang und Authentisierung ... 457
18.2.1 Sicherer lokaler Zugang ... 457
18.2.2 Sicherer Fernzugang ... 461
18.2.3 Session-Sicherheit ... 462

18.3 Schutz der Anwenderdaten ... 463
18.3.1 Ablage auf Speichermedien ... 463
18.3.2 Verarbeitung im Speicher ... 464
18.3.3 Transit über ein Netzwerk ... 464

18.4 Konfigurationsmanagement ... 465

18.5 Protokollierung und Überwachung ... 465
18.5.1 Protokollierung und Auswertung ... 465
18.5.2 Überwachung im laufenden Betrieb ... 468

18.6 Selbstschutz des Betriebssystems ... 470
18.6.1 Härtung gegen spezifische Bedrohungen ... 470
18.6.2 Malwareschutz ... 473
18.6.3 Boot-Schutz ... 473
18.6.4 Verwaltung angeschlossener Geräte und Speichermedien ... 474
18.6.5 Reduktion der Angriffsoberfläche ... 475
18.6.6 Einschränkung des zulässigen Netzwerkverkehrs ... 475

19 Löschen und Entsorgen 477

19.1 Anforderungen zum Löschen und Entsorgen ... 477

19.2 Lösch- und Entsorgungskonzept ... 479
19.2.1 Speicherorte ... 480
19.2.2 Angemessene Löschstrategien ... 483
19.2.3 Verantwortlichkeiten und Integration in den Arbeitsalltag ... 483

19.3 Technische Löschmaßnahmen ... 484
19.3.1 Einfaches Löschen ... 484
19.3.2 Sicheres Löschen ... 485
19.3.3 Verschlüsselung und Löschen ... 485
19.3.4 Löschen auf USB-Sticks und anderen Flash-Medien ... 486
19.3.5 Vernichten und Entsorgen ... 487

20 Sicherheit in World Wide Web und E-Commerce 493

20.1 Bedrohungen und Sicherheitsmaßnahmen im Web ... 493
20.1.1 Einführung in Web-Anwendungen ... 493
20.1.2 Ausgewählte Angriffe ... 498
20.1.3 Sicherung von Web-Anwendungen ... 501
20.1.4 Phishing ... 502

20.2 E-Commerce und E-Payment ... 503
20.2.1 Online-Banking ... 503
20.2.2 Elektronische Bezahlverfahren ... 506

21 Awareness 509

21.1 „Risikofaktor“ Mensch 509
21.1.1 Zur Wahrnehmung von IT-Sicherheit 510
21.1.2 Randbedingungen und Konsequenzen 511
21.2 Durchführung von Awareness-Kampagnen 512
21.2.1 Kampagnen-Problematiken 512
21.2.2 Zielsetzung einer Awareness-Kampagne 513
21.3 Awareness in der Praxis 515
21.3.1 Erfolgsfaktoren 515
21.3.2 Beteiligte 516
21.3.3 Das Vier-Phasen-Konzept einer Awareness-Kampagne 517
21.3.4 Erfolgsmessung 521

22 Computer-Viren und Content Security 523

22.1 Verbreitungswege von Malware 523
22.2 Unerwünschte Inhalte 524
22.2.1 Klassen von „Malicious Code“ 524
22.2.2 Spam 525
22.2.3 Aktive Inhalte 526
22.2.4 Bedrohungen durch Malware 527
22.3 Ansätze zur Abwehr von Malware 529
22.4 Abschottung von Systemen 530
22.5 Content-Analyse 530
22.5.1 Erfassung des Netzwerkverkehrs 532
22.5.2 Dekomposition der Inhalte und Header-Analyse 534
22.5.3 Klassifikation von Inhalten 534
22.5.4 Aktion 535
22.5.5 Besonderheiten bei Anti-Spam-Maßnahmen 536
22.5.6 Content-Filter und verschlüsselte Inhalte 538
22.6 Verhaltensanalyse 539

23 Intrusion Detection 541

23.1 Einordnung und Definitionen 541
23.2 Architektur und Komponenten von Intrusion-Detection-Systemen 542
23.3 Grundproblem der Analyse – oder „der Schein trügt“ 544
23.4 Typen von Intrusion-Detection-Systemen 545
23.4.1 Host-based Intrusion-Detection-Systeme 545
23.4.2 Network-based Intrusion-Detection-System 546
23.4.3 Hybride Intrusion-Detection-Systeme 546
23.5 Komponenten von Intrusion-Detection-Systemen 547
23.5.1 Hostsensoren 547
23.5.2 Netzsensoren 547
23.5.3 Datenbankkomponenten 548

23.5.4 Managementstation *548*
23.5.5 Auswertungsstation *549*
23.6 Methoden der Angriffserkennung 549
23.6.1 Erkennen von Angriffsmustern *549*
23.6.2 Anomalieerkennung *550*
23.6.3 Korrelation von Ereignisdaten *550*
23.7 Das Intrusion-Detection-Dilemma 550
23.8 Ausblick und Vorgaben für IDS 552
23.8.1 Anforderungen an die Sicherheitsadministration *552*
23.8.2 Auswahl und Test eines IDS *553*

24 Datensicherung 555

24.1 Zwecke der Datensicherung 555
24.2 Strategien der Datensicherung 556
24.3 Backups von vertraulichen Daten 559
24.4 Backup-Medien 559
24.5 Erfolgsfaktoren für Recovery 560
24.5.1 Physische Verfügbarkeit *560*
24.5.2 Betriebliche Voraussetzungen für Recovery *561*
24.5.3 Recovery-Fähigkeit überprüfen *561*
24.6 Datensicherungskonzept 562

25 Incident-Management und Computer Emergency Response Teams 565

25.1 Ziel und Aufgaben des Incident-Management 565
25.2 Der Aufbau des CERT 566
25.3 Regelmäßige Aufgaben des CERT 571
25.3.1 Überwachen der Informationsströme – Erkennen von Incidents *571*
25.3.2 Aufbau- und Pflegearbeiten *573*
25.4 Der Incident-Prozess 574
25.4.1 Phase 1: Analysieren *574*
25.4.2 Phase 2: Reagieren *578*
25.4.3 Phase 3: Nachbereitung *580*

26 Business-Continuity-Management 585

26.1 Business Continuity 585
26.1.1 Hohe Verfügbarkeit erreichen und schwere Störfälle beherrschen *585*
26.1.2 Business-Impact-Analyse *586*
26.1.3 Verantwortung für Business Continuity *591*
26.2 Business Continuity vorbereiten 591
26.2.1 Notfall-Teams und Krisenstab etablieren *592*
26.2.2 Störfall-Eskalationswege aufbauen *593*

26.2.3 Notfallhandbuch bereitstellen ... 594
26.2.4 Notfallvorsorge ... 596
26.2.5 Krisenkommunikation vorbereiten ... 598
26.2.6 BC-Training, BC-Awareness, und BC-Kultur ... 598

26.3 BCM etablieren ... 599
26.3.1 Das BCM-Team ... 600
26.3.2 Initialisierung des Business-Continuity-Management ... 600
26.3.3 BCM-Planungsphase ... 601
26.3.4 Umsetzungsphase ... 602
26.3.5 Überwachung ... 603
26.3.6 Weiterentwicklung ... 603

26.4 Standards für BCM ... 604
26.4.1 ISO 22301 ... 604
26.4.2 ISO 22313 ... 606
26.4.3 ISO/IEC 27031 ... 606
26.4.4 BSI-Standard 100-4 Notfallmanagement ... 607
26.4.5 BCI Good Practice Guidelines ... 608

Verzeichnis der Autoren **611**

Übersicht zu Standards der Informationssicherheit **615**

Abbildungsverzeichnis **647**

Abkürzungen und Glossar **649**

Index **673**