Mathias Gut

Markus Kammermann

4. Auflage

mitp

CompTIA Security+

IT-Sicherheit verständlich erklärt

Die umfassende Prüfungsvorbereitung zur CompTIA-Prüfung SY0-601

Inhaltsverzeichnis

1	**Laras Welt**	23
1.1	Das Ziel dieses Buches	24
1.2	Die CompTIA Security+-Zertifizierung	25
1.3	Voraussetzungen für CompTIA Security+	27
1.4	Persönliches	27
2	**Sind Sie bereit für CompTIA Security+?**	31
3	**Wo liegt denn das Problem?**	39
3.1	Fangen Sie bei sich selbst an	39
3.2	Die Gefahrenlage	41
3.3	Die Analyse der Bedrohungslage	44
3.4	Kategorien der Informationssicherheit	44
3.5	Modelle und Lösungsansätze	47
3.5.1	TCSEC oder ITSEC	47
3.5.2	Common Criteria	48
3.5.3	ISO 27000	50
3.5.4	Das NIST Cybersecurity Framework	50
3.6	Der IT-Grundschutz nach BSI	52
3.7	Lösungsansätze für Ihr Unternehmen	55
3.7.1	Das Information Security Management System	57
3.7.2	Sicherheitsmanagement und Richtlinien	57
3.7.3	Die Notfallvorsorge	58
3.7.4	Risiken durch Dritte	59
3.7.5	Die Cyber-Security-Strategie	60
3.8	Fragen zu diesem Kapitel	62
4	**Rechtliche Grundlagen**	65
4.1	Warum ist Datenschutz für Sie relevant?	66
4.1.1	Die Ursprünge des Datenschutzes	67
4.1.2	Datenschutz-Compliance für Unternehmen	68
4.1.3	Datenschutz als Beruf	69
4.2	Was sind Personendaten?	70
4.2.1	Relativer vs. absoluter Ansatz	70
4.2.2	Was sind Personendaten nach relativem Ansatz?	71

4.2.3 Anonymisierte und pseudonymisierte Daten 71
4.2.4 Anwendungsbeispiele 71
4.2.5 Besonders sensible Daten 72
4.3 Was hat Datenschutz mit Datensicherheit zu tun? 73
4.3.1 Was bedeuten die gesetzlichen Vorgaben für die Praxis? . . . 74
4.3.2 Data Breach Notifications. 76
4.3.3 Datenschutzfreundliches Design und ebensolche Konfiguration 76
4.3.4 Haftungsrisiko bei Missachtung der Datensicherheit 76
4.4 Inwiefern wird Missbrauch von Daten unter Strafe gestellt? 78
4.4.1 Unbefugte Datenbeschaffung (sog. Datendiebstahl) 78
4.4.2 Unbefugtes Eindringen in ein Datenverarbeitungssystem 78
4.4.3 Datenbeschädigung 79
4.4.4 Betrügerischer Missbrauch einer Datenverarbeitungsanlage. 79
4.4.5 Erschleichen einer Leistung. 80
4.4.6 Unbefugte Entschlüsselung codierter Angebote 80
4.4.7 Unbefugtes Beschaffen von Personendaten 80
4.4.8 Phishing und Skimming 81
4.4.9 Verletzung von Berufs-, Fabrikations- und Geschäftsgeheimnissen 81
4.4.10 Massenversand von Werbung (Spam) 82
4.5 Wann ist welches Gesetz anwendbar? 82
4.5.1 Sachlicher Anwendungsbereich 83
4.5.2 Räumlicher Anwendungsbereich 83
4.6 Welche Grundsätze müssen eingehalten werden? 86
4.7 Der Grundsatz der Datenminimierung 87
4.7.1 Unterschied zwischen Datensicherung und -archivierung 88
4.7.2 Weshalb müssen Daten gesichert und archiviert werden? 88
4.7.3 Verwaltung der zu sichernden und zu archivierenden Daten 89
4.7.4 Wie werden nicht mehr benötigte Daten sicher vernichtet? 89
4.8 Welche Rechte haben die betroffenen Personen? 90
4.8.1 Recht auf Information 90

4.8.2 Recht auf Auskunft ... 91
4.8.3 Berichtigung, Einschränkung und Löschung ... 92
4.8.4 Recht auf Datenübertragbarkeit ... 92
4.8.5 Widerspruchsrecht ... 93
4.8.6 Beschwerderecht ... 94
4.9 Was ist bei der Zusammenarbeit mit Dritten zu beachten? ... 95
4.9.1 Auftragsbearbeiter ... 95
4.9.2 Gemeinsame Verantwortliche ... 96
4.9.3 Bearbeitung im Konzern ... 96
4.9.4 Datenexporte ... 96
4.10 Haftungsrisiken bei Datenschutzverletzungen ... 98
4.11 Fragen zu diesem Kapitel ... 101

5 Verschlüsselungstechnologie ... 103
5.1 Grundlagen der Kryptografie ... 104
5.1.1 Einige Grundbegriffe ... 105
5.1.2 One-Time-Pad ... 105
5.1.3 Diffusion und Konfusion ... 106
5.1.4 Blockverschlüsselung ... 107
5.1.5 Stromverschlüsselung ... 108
5.2 Symmetrische Verschlüsselung ... 109
5.2.1 DES ... 110
5.2.2 3DES ... 110
5.2.3 AES ... 111
5.2.4 Blowfish ... 111
5.2.5 Twofish ... 112
5.2.6 RC4 ... 112
5.3 Asymmetrische Verschlüsselung ... 112
5.3.1 RSA ... 114
5.3.2 Diffie-Hellman ... 114
5.3.3 ECC ... 115
5.3.4 Perfect Forward Secrecy (PFS) ... 116
5.3.5 Die Zukunft der Quanten ... 116
5.4 Hash-Verfahren ... 116
5.4.1 MD4 und MD5 ... 118
5.4.2 SHA ... 118
5.4.3 RIPEMD ... 119
5.4.4 HMAC ... 119
5.4.5 Hash-Verfahren mit symmetrischer Verschlüsselung ... 120

5.4.6 Digitale Signaturen 120
5.4.7 Hybride Verschlüsselung 120
5.5 Drei Status digitaler Daten 122
5.5.1 Data-in-transit 122
5.5.2 Data-at-rest 122
5.5.3 Data-in-use 123
5.6 Bekannte Angriffe gegen die Verschlüsselung 123
5.6.1 Cipher-text-only-Angriff 123
5.6.2 Known/Chosen-plain-text-Angriff 123
5.6.3 Schwache Verschlüsselung / Implementierung 124
5.6.4 Probleme mit Zertifikaten 124
5.7 PKI in Theorie und Praxis 124
5.7.1 Aufbau einer hierarchischen PKI 126
5.7.2 SSL-Zertifikate X.509 Version 3 127
5.7.3 Zertifikatstypen 128
5.7.4 Zurückziehen von Zertifikaten 131
5.7.5 Hinterlegung von Schlüsseln 131
5.7.6 Aufsetzen einer hierarchischen PKI 132
5.8 Fragen zu diesem Kapitel 132

6 Die Geschichte mit der Identität 135
6.1 Identitäten und deren Rechte 135
6.1.1 Zuweisung von Rechten 135
6.1.2 Rollen 137
6.1.3 Single Sign On 137
6.2 Authentifizierungsmethoden 137
6.2.1 Benutzername und Kennwort 138
6.2.2 Token 139
6.2.3 Zertifikate 139
6.2.4 Biometrie 140
6.2.5 Benutzername, Kennwort und Smartcard 142
6.2.6 Tokenization 143
6.2.7 Wechselseitige Authentifizierung 144
6.3 Zugriffssteuerungsmodelle 144
6.3.1 Mandatory Access Control (MAC) 144
6.3.2 Discretionary Access Control (DAC) 146
6.3.3 Role Based Access Control (RBAC) 146
6.3.4 ABAC – Attributbasiertes Zugriffssystem 148
6.3.5 Principle of Least Privileges 149

6.4 Protokolle für die Authentifizierung ... 149
6.4.1 Kerberos ... 149
6.4.2 PAP ... 150
6.4.3 CHAP ... 150
6.4.4 NTLM ... 151
6.4.5 Die Non-Repudiation ... 151
6.5 Vom Umgang mit Passwörtern ... 152
6.6 Fragen zu diesem Kapitel ... 153

7 Physische Sicherheit ... 157
7.1 Zutrittsregelungen ... 158
7.1.1 Das Zonenkonzept ... 159
7.1.2 Schlüsselsysteme ... 160
7.1.3 Badges und Keycards ... 160
7.1.4 Biometrische Erkennungssysteme ... 161
7.1.5 Zutrittsschleusen ... 162
7.1.6 Videoüberwachung ... 163
7.1.7 Multiple Systeme ... 164
7.2 Bauschutz ... 164
7.2.1 Einbruchsschutz ... 164
7.2.2 Hochwasserschutz ... 165
7.2.3 Brandschutz ... 165
7.2.4 Klimatisierung und Kühlung ... 167
7.3 Elektrostatische Entladung ... 169
7.4 Stromversorgung ... 170
7.4.1 USV ... 170
7.4.2 Notstromgruppen ... 172
7.4.3 Einsatzszenarien ... 173
7.4.4 Rotationsenergiestromversorgungen ... 174
7.4.5 Ein Wort zu EMP ... 175
7.5 Feuchtigkeit und Temperatur ... 175
7.6 Fragen zu diesem Kapitel ... 177

8 Im Angesicht des Feindes ... 179
8.1 Malware ist tatsächlich böse ... 180
8.1.1 Die Problematik von Malware ... 184
8.1.2 Viren und ihre Unterarten ... 186
8.1.3 Wie aus Trojanischen Pferden böse Trojaner wurden ... 189
8.1.4 Backdoor ... 193

8.1.5 Logische Bomben 193
8.1.6 Würmer 194
8.1.7 Ransomware 195
8.1.8 Krypto-Malware (Cryptomalware) 197
8.1.9 Fileless Malware 198
8.1.10 Hoaxes 198
8.2 Angriffe mittels Social Engineering 199
8.2.1 Phishing 199
8.2.2 Vishing und Smishing 203
8.2.3 Spear Phishing 204
8.2.4 Pharming 205
8.2.5 Drive-by-Pharming 205
8.2.6 Doxing 206
8.3 Angriffe gegen IT-Systeme 206
8.3.1 Exploits und Exploit-Kits 207
8.3.2 Darknet und Darkweb 209
8.3.3 Malwaretising 210
8.3.4 Watering-Hole-Attacke 210
8.3.5 Malware Dropper und Malware-Scripts 210
8.3.6 RAT (Remote Access Tool/Remote Access Trojan) 211
8.3.7 Keylogger 211
8.3.8 Post Exploitation 213
8.4 Gefahren für die Nutzung mobiler Geräte und Dienste 214
8.5 APT – Advanced Persistent Threats 216
8.5.1 Carbanak 217
8.6 Advanced Threats 218
8.6.1 Evasion-Techniken 219
8.6.2 Pass-the-Hash-Angriffe (PtH) 220
8.6.3 Kaltstartattacke (Cold Boot Attack) 221
8.6.4 Physische RAM-Manipulation über DMA (FireWire-Hack) 221
8.6.5 Human Interface Device Attack (Teensy USB HID Attack) 221
8.6.6 BAD-USB-Angriff 222
8.6.7 Bösartiges USB-Kabel 222
8.6.8 SSL-Stripping-Angriff 223
8.6.9 Angriff über Wireless-Mäuse 223

8.7 Angriffe in Wireless-Netzwerken 224
8.7.1 Spoofing in Wireless-Netzwerken 225
8.7.2 Sniffing in drahtlosen Netzwerken 225
8.7.3 DNS-Tunneling in Public WLANs 227
8.7.4 Rogue Access Point/Evil Twin 228
8.7.5 Attacken auf die WLAN-Verschlüsselung 229
8.7.6 Verschlüsselung brechen mit WPS-Attacken 230
8.7.7 Denial-of-Service-Angriffe im WLAN 231
8.7.8 Angriffe auf NFC-Technologien 231
8.7.9 Angriffe auf Keycards 232
8.8 Moderne Angriffsformen 233
8.8.1 Angriffe mittels Drohnen 233
8.8.2 Verwundbare Anwendungen nachladen 234
8.8.3 Angriffe auf Application Programming Interface (API) 234
8.8.4 Gefahren durch künstliche Intelligenz (KI) 234
8.8.5 Das Internet of Things 235
8.9 Fragen zu diesem Kapitel 237

9 Systemsicherheit realisieren 241
9.1 Konfigurationsmanagement 242
9.2 Das Arbeiten mit Richtlinien 244
9.3 Grundlagen der Systemhärtung 246
9.3.1 Schutz von Gehäuse und BIOS 248
9.3.2 Sicherheit durch TPM 250
9.3.3 Full Disk Encryption 250
9.3.4 Softwarebasierte Laufwerksverschlüsselung 251
9.3.5 Hardware-Sicherheitsmodul 251
9.3.6 Software-Firewall (Host-based Firewall) 252
9.3.7 Systemintegrität 252
9.3.8 Überlegungen bei der Virtualisierung 253
9.4 Embedded-Systeme und Industriesysteme 254
9.5 Softwareaktualisierung ist kein Luxus 259
9.5.1 Vom Hotfix zum Upgrade 261
9.5.2 Problemkategorien 262
9.5.3 Maintenance-Produkte 262
9.5.4 Die Bedeutung des Patch- und Update-Managements 264
9.5.5 Entfernen Sie, was Sie nicht brauchen 265
9.6 Malware bekämpfen 266
9.6.1 Endpoint-Protection am Client 269

9.6.2 Reputationslösungen 270
9.6.3 Aktivitätsüberwachung HIPS/HIDS 270
9.6.4 Online-Virenscanner – Webantivirus-NIPS 271
9.6.5 Sensibilisierung der Mitarbeitenden 271
9.6.6 Suchen und Entfernen von Viren 273
9.6.7 Virenschutzkonzept 274
9.6.8 Testen von Installationen 276
9.6.9 Sicher und vertrauenswürdig ist gut 276
9.7 Advanced Threat Protection 278
9.7.1 Explizites Applikations-Whitelisting versus -Blacklisting . . . 278
9.7.2 Explizites Whitelisting auf Firewalls 279
9.7.3 Erweiterter Exploit-Schutz 280
9.7.4 Virtualisierung von Anwendungen 282
9.7.5 Schutz vor HID-Angriffen und BAD-USB 282
9.7.6 Geschlossene Systeme 284
9.7.7 Schutz vor SSL-Stripping-Angriffen 285
9.7.8 Schutz vor Angriffen über drahtlose Mäuse 287
9.7.9 Security- und Threat Intelligence 288
9.8 Anwendungssicherheit 289
9.8.1 Lifecycle-Management/DevOps 289
9.8.2 Sichere Codierungskonzepte 290
9.8.3 Input Validation 290
9.8.4 Fehler- und Ausnahmebehandlung 290
9.8.5 Memory Leak 290
9.8.6 NoSQL- versus SQL-Datenbanken 291
9.8.7 Serverseitige versus clientseitige Validierung 291
9.8.8 Session Token 292
9.8.9 Web-Application-Firewall (WAF) 292
9.9 Fragen zu diesem Kapitel 292

10 Sicherheit für mobile Systeme 295
10.1 Die Risikolage mit mobilen Geräten und Diensten 296
10.2 Organisatorische Sicherheitsmaßnahmen 296
10.3 Technische Sicherheitsmaßnahmen 297
10.3.1 Vollständige Geräteverschlüsselung (Full Device Encryption) 299
10.3.2 Gerätesperren (Lockout) 300
10.3.3 Bildschirmsperre (Screenlocks) 301
10.3.4 Remote Wipe/Sanitization 301

10.3.5 Standortdaten (GPS) und Asset Tracking 301
10.3.6 Sichere Installationsquellen und Anwendungssteuerung 302
10.3.7 VPN-Lösungen auf mobilen Geräten 303
10.3.8 Public-Cloud-Dienste auf mobilen Geräten 303
10.4 Anwendungssicherheit bei mobilen Systemen 303
10.4.1 Schlüsselverwaltung (Key-Management) 304
10.4.2 Credential-Management 304
10.4.3 Authentifizierung 304
10.4.4 Geo-Tagging 305
10.4.5 Verschlüsselung 305
10.4.6 Whitelisting von Anwendungen 305
10.4.7 Transitive Trust/Authentifizierung 305
10.5 Fragen rund um BYOD 306
10.5.1 Dateneigentum (Data Ownership) 306
10.5.2 Zuständigkeit für den Unterhalt (Support Ownership) 307
10.5.3 Antivirus-Management 307
10.5.4 Patch-Management 307
10.5.5 Forensik 308
10.5.6 Privatsphäre und Sicherheit der geschäftlichen Daten 308
10.5.7 Akzeptanz der Benutzer und akzeptable Benutzung 309
10.5.8 Architektur-/Infrastrukturüberlegungen 310
10.5.9 On-Board-Kamera/Video 310
10.6 Fragen zu diesem Kapitel 310

11 Den DAU gibt's wirklich – und Sie sind schuld 313
11.1 Klassifizierung von Informationen 314
11.1.1 Die Klassifizierung nach Status 314
11.1.2 Die Klassifizierung nach Risiken 316
11.1.3 Data Loss Prevention 318
11.1.4 Was es zu beachten gilt 319
11.2 Der Datenschutz im internationalen Umfeld 319
11.3 Vom Umgang mit dem Personal 323
11.4 Umgang mit Social Engineering 326
11.4.1 Praktiken, Ziele und Vorgehensweisen von Social Engineers 326
11.4.2 Informationsbeschaffung von OSINT bis Dumpster Diving 327
11.4.3 Pretexting und authentische Geschichten 328

11.4.4 Shoulder surfing 330
11.4.5 Tailgating 331
11.4.6 Gezielte Beeinflussung und Falschinformation (Influence campaigns) 332
11.4.7 CEO Fraud / Rechnungsbetrug 332
11.4.8 Prepending 332
11.4.9 Awareness-Schulungen und Reglements 333
11.5 E-Mail-Sicherheit 333
11.5.1 Secure Multipurpose Internet Mail Extensions (S/MIME) 334
11.5.2 PGP (Pretty Good Privacy) 335
11.5.3 Schwachstellen 338
11.5.4 Schutz durch einen Mail-Gateway 342
11.5.5 Social Media 342
11.6 Daten sichern 343
11.6.1 Datensicherung oder Datenarchivierung? 345
11.6.2 Die gesetzlichen Grundlagen 346
11.6.3 Das Datensicherungskonzept 348
11.6.4 Methoden der Datensicherung 352
11.6.5 Online-Backup 355
11.6.6 Daten vernichten 357
11.7 Sicherheit im Umgang mit Servicepartnern 357
11.8 Fragen zu diesem Kapitel 359

12 Sicherheit für Netzwerke 363
12.1 Trennung von IT-Systemen 363
12.1.1 Subnettierung von Netzen 364
12.1.2 NAT 366
12.1.3 Network Access Control 367
12.2 VLAN 368
12.2.1 Planung und Aufbau von VLANs 368
12.2.2 Vorgehen gegen Risiken bei Switch-Infrastrukturen 372
12.2.3 Port Security 373
12.2.4 Flood Guard 373
12.2.5 Spanning-Tree Protocol und Loop Protection 374
12.2.6 Maßnahmen gegen Gefahren in VLANs 375
12.3 TCP/IP-Kernprotokolle 376
12.3.1 Internet Protocol 376
12.3.2 Internet Control Message Protocol 376

12.3.3 Transmission Control Protocol 377
12.3.4 User Datagram Protocol (UDP) 378
12.4 Weitere Transport- und Netzwerkprotokolle 378
12.4.1 Address Resolution Protocol (ARP) 378
12.4.2 Internet Group Management Protocol (IGMP) 379
12.4.3 SLIP und PPP 379
12.4.4 IP-Version 6 379
12.4.5 Portnummern 380
12.5 Anwendungen 380
12.5.1 Telnet und SSH 381
12.5.2 FTP und TFTP 381
12.5.3 SCP, SFTP und FTPS 381
12.5.4 DNS 382
12.5.5 SNMP 383
12.5.6 E-Mail-Protokolle 383
12.5.7 HTTP 383
12.5.8 SSL und TLS 384
12.5.9 NetBIOS und CIFS 387
12.5.10 Lightweight Directory Access (LDAP) 387
12.6 Sicherheit in der Cloud 388
12.6.1 Cloud-Computing-Betriebsmodelle 389
12.6.2 Sicherheit in der Wolke 390
12.6.3 Formen des Einsatzes 391
12.7 Fragen zu diesem Kapitel 393

13 Schwachstellen und Attacken 395
13.1 Welches Risiko darf es denn sein? 395
13.2 Angriffe gegen IT-Systeme 397
13.2.1 Denial of Service 397
13.2.2 Pufferüberlauf 398
13.2.3 Race-Condition 399
13.2.4 Password Guessing und Cracking 399
13.3 Angriffe gegen Anwendungen 401
13.3.1 Directory-Traversal 401
13.3.2 Cross Site Scripting 403
13.3.3 Cross-Site Request Forgery (XSRF) 403
13.3.4 Injection-Varianten 404
13.3.5 Parametermanipulation 405
13.3.6 Transitive Zugriffe 406

13.3.7 Phishing 406
13.3.8 Treibermanipulationen 407
13.4 Angriffe gegen Clients 407
13.4.1 Drive by Attack 408
13.4.2 Böswillige Add-ons und Applets 408
13.4.3 Local Shared Objects (LSOs) 408
13.4.4 Spam, Spim und Spit 409
13.4.5 Typo squatting bzw. URL-Hijacking 409
13.4.6 URL-Redirection 410
13.4.7 Clickjacking 410
13.4.8 Domain Hijacking 410
13.4.9 Man in the Browser 410
13.5 Netzwerkangriffe 410
13.5.1 Denial of Service (DoS) 410
13.5.2 Distributed Denial of Service (DDoS) 412
13.5.3 Spoofing 413
13.5.4 Man in the Middle 414
13.5.5 Replay-Angriff 416
13.5.6 SSL-Downgrading 417
13.5.7 Session-Hijacking 417
13.5.8 Brechen von Schlüsseln 418
13.5.9 Backdoor 419
13.6 Angriffe gegen die Public Cloud 419
13.7 Steganografie 420
13.8 Akteure und ihre Motive 421
13.8.1 Generelle Eigenschaften der verschiedenen Angreifer 422
13.8.2 Von Hüten und Angreifern 423
13.8.3 Staatliche Akteure (State actors) 424
13.8.4 Organisierte Kriminalität (Criminal syndicates) 425
13.8.5 Wirtschaftsspionage (Competitors) und interne Täter 425
13.8.6 Hacktivisten (Hacktivists) 425
13.8.7 Script-Kiddies 426
13.8.8 Die Schatten-IT (Shadow IT) 426
13.8.9 Bug-Bounty 427
13.9 Fragen zu diesem Kapitel 427

14 Der sichere Remote-Zugriff 431
14.1 Virtual Private Network 431
14.1.1 Site-to-Site-VPN 433

14.1.2 Remote-Access-VPN 434
14.1.3 Soft- und Hardwarelösungen 435
14.2 Remote Access Server 436
14.3 Protokolle für den entfernten Zugriff 436
14.3.1 802.1x 436
14.3.2 RADIUS 438
14.3.3 TACACS, XTACACS und TACACS+ 439
14.3.4 L2TP und PPTP 440
14.3.5 IPsec 441
14.3.6 SSL/TLS 447
14.3.7 SSH 447
14.3.8 SRTP 449
14.4 Schwachstellen 449
14.5 Fragen zu diesem Kapitel 450

15 Drahtlose Netzwerke sicher gestalten 453
15.1 Aller WLAN-Standard beginnt mit IEEE 802.11 454
15.1.1 Die frühen IEEE-Standards von 802.11 454
15.1.2 Die Gegenwart heißt Wi-Fi 6 456
15.2 Die Verbindungsaufnahme im WLAN 459
15.2.1 Das Ad-hoc-Netzwerk 459
15.2.2 Das Infrastrukturnetzwerk 460
15.2.3 Erweitertes Infrastrukturnetz 460
15.3 Ein WLAN richtig aufbauen 461
15.3.1 Aufbau der Hardware 461
15.3.2 Konfiguration des drahtlosen Netzwerks 463
15.4 Sicherheit in drahtlosen Verbindungen 465
15.4.1 Wired Equivalent Privacy 466
15.4.2 Von WPA bis WPA3 468
15.4.3 Die Implementierung von 802.1x 470
15.4.4 Das Extensible Authentication Protocol (EAP) 471
15.4.5 WAP (Wireless Application Protocol) 472
15.4.6 Near Field Communication 473
15.5 Grundlegende Sicherheitsmaßnahmen umsetzen 474
15.6 Wireless Intrusion Prevention System 476
15.7 Bluetooth – Risiken und Maßnahmen 476
15.8 Fragen zu diesem Kapitel 478

16 System- und Netzwerküberwachung 481
16.1 Das OSI-Management-Framework 481
16.2 SNMP-Protokolle 484
16.3 Leistungsüberwachung 487
16.4 Das Monitoring von Netzwerken 489
16.5 Monitoring-Programme 490
16.5.1 Der Windows-Netzwerkmonitor 490
16.5.2 Wireshark 492
16.5.3 inSSIDer 495
16.5.4 MRTG bzw. RRDTools 495
16.5.5 Nagios 497
16.6 Proaktive Sicherheit dank SIEM 498
16.7 Kommandozeilenprogramme 500
16.7.1 ipconfig/ip 500
16.7.2 ping 502
16.7.3 ARP 503
16.7.4 tracert/traceroute 504
16.7.5 nslookup 505
16.7.6 netstat 506
16.8 Fragen zu diesem Kapitel 507

17 Brandschutzmauer für das Netzwerk 511
17.1 Damit kein Feuer ausbricht 511
17.2 Personal Firewalls und dedizierte Firewalls 513
17.3 Das Regelwerk einer Firewall 515
17.3.1 Positive Exceptions (Positive Rules) 515
17.3.2 Negative Exceptions (Negative Rules) 515
17.4 Das Konzept der DMZ 516
17.4.1 Trennung Hostsystem von den virtuellen Maschinen 518
17.4.2 Trennung bei WLAN-Infrastrukturen 518
17.4.3 Extranet und Intranet 519
17.5 Nicht jede Firewall leistet dasselbe 519
17.5.1 Wenn einfach auch reicht: Die Paketfilter-Firewall 519
17.5.2 Der nächste Level: Stateful Packet Inspection Firewall 520
17.5.3 Jetzt wird's gründlich: Application Level Gateway 521
17.5.4 Anwendungsbeispiele 523
17.5.5 Unified Threat Management Firewall 525
17.6 Die Angreifer kommen – aber Sie wissen's schon 525

17.7 Unified Threat Management 528
17.8 Fragen zu diesem Kapitel 530

18 Sicherheit überprüfen und analysieren 533
18.1 Informationsbeschaffung 534
18.1.1 Branchen- und Interessensverbände 534
18.1.2 Fachmedien 534
18.1.3 Schwachstelleninformationen 535
18.1.4 Sicherheitskonferenzen 535
18.1.5 Hersteller-Webseiten 535
18.2 Penetration Testing 535
18.2.1 Organisatorische Einbettung 537
18.2.2 Prinzipielle Vorgehensweise 539
18.2.3 Black Box und White Box 543
18.2.4 Security-Scanner 544
18.2.5 Datenbanken für Recherchen nach Sicherheitslücken 547
18.2.6 Passwort-Guesser und -Cracker 547
18.2.7 Paketgeneratoren und Netzwerk-Sniffer 549
18.2.8 Fuzzing 550
18.2.9 Metasploit Framework 550
18.3 Forensik 551
18.3.1 Vorbereitung 552
18.3.2 Sichern von Beweismitteln 553
18.3.3 Beweissicherung nach RFC 3227 554
18.3.4 Schutz und Analyse von Beweismitteln 555
18.3.5 Timeline 557
18.3.6 Data-Carving 557
18.3.7 Suche nach Zeichenketten 558
18.3.8 Nutzung von Hash-Datenbanken 558
18.3.9 Programme und Toolkits 559
18.4 Fragen zu diesem Kapitel 561

19 Wider den Notfall 563
19.1 Was ist denn ein Notfall? 564
19.2 Resilienz dank Fehlertoleranz 565
19.2.1 Aller Anfang ist RAID 566
19.2.2 RAID Level 567
19.2.3 Duplexing 572
19.2.4 Übersicht RAID 572

19.3 Redundante Verbindungen und Systeme 573
19.3.1 Network Loadbalancing 573
19.3.2 Cluster 574
19.4 Notfallvorsorgeplanung 575
19.4.1 Bedrohungsanalyse 575
19.4.2 Von der Bedrohung bis zur Maßnahme 576
19.5 Ein guter Plan beginnt mit einer guten Analyse 577
19.5.1 Ausfallszenarien 577
19.5.2 Impact-Analyse 577
19.6 Methoden der Umsetzung 579
19.6.1 Strategie und Planung 579
19.6.2 Die Rolle des Risiko-Managements 581
19.6.3 Verschiedene Implementierungsansätze 583
19.6.4 Incident-Response-Prozesse und Incident Response Plan 585
19.7 Test und Wartung des Notfallplans 587
19.7.1 Wartung der Disaster Recovery 587
19.7.2 Punktuelle Anpassungen 587
19.7.3 Regelmäßige Überprüfung 588
19.7.4 Merkpunkte zur Datenwiederherstellung 588
19.8 Fragen zu diesem Kapitel 589

20 Security-Audit 593
20.1 Grundlagen von Security-Audits 594
20.1.1 Fragestellungen 594
20.1.2 Prinzipielle Vorgehensweise 594
20.1.3 Bestandteile eines Security-Audits 595
20.2 Standards 595
20.2.1 ISO 27001 596
20.2.2 IT-Grundschutz nach BSI 596
20.2.3 Kombination aus ISO 27000 und IT-Grundschutz 597
20.3 Beispiel-Audit Windows Server 2019 597
20.3.1 Nutzung von Sicherheitsvorlagen 598
20.3.2 Einsatz von Kommandos und Scripts 598
20.3.3 Passwortschutz 598
20.3.4 Geräteschutz 598
20.3.5 Sichere Basiskonfiguration 599
20.3.6 Sichere Installation und Bereitstellung 599
20.3.7 Sichere Konfiguration der IIS-Basis-Komponente 599

20.3.8 Sichere Migration auf Windows Server 2019 599
20.3.9 Umgang mit Diensten unter Windows Server 600
20.3.10 Deinstallation nicht benötigter Client-Funktionen 600
20.3.11 Verwendung der Softwareeinschränkungsrichtlinie 600
20.4 Berichtswesen 600
20.4.1 Titelseite 601
20.4.2 Einleitung 601
20.4.3 Management-Summary 601
20.4.4 Ergebnisse der Untersuchung 601
20.4.5 Erforderliche Maßnahmen 602
20.4.6 Anhang 602
20.5 Ergänzende Maßnahmen 603
20.5.1 Logfile-Analyse 603
20.5.2 Echtzeitanalyse von Netzwerkverkehr und Zugriffen 604
20.5.3 Risikoanalyse 604
20.6 Fragen zu diesem Kapitel 605

21 Die CompTIA Security+-Prüfung 607
21.1 Was von Ihnen verlangt wird 608
21.2 Wie Sie sich vorbereiten können 609
21.3 Wie eine Prüfung aussieht 609
21.4 Beispielprüfung zum Examen CompTIA Security+ 614

A Anhänge 633
A.1 Antworten zu den Vorbereitungsfragen 633
A.2 Antworten zu den Kapitelfragen 633
A.3 Antworten zu Fragen der Beispielprüfung 635
A.4 Weiterführende Literatur 636
A.4.1 Nützliche Literatur zum Thema 636
A.4.2 Weiterführende Links zum Thema 637

B Abkürzungsverzeichnis 639

Stichwortverzeichnis 653

Kapitel 1

Laras Welt

Guten Tag, ich bin Lara aus Neustadt. Ich arbeite bei der lokalen Agentur der Nixsicura-Versicherungen und möchte euch einen Einblick in meinen beruflichen Alltag und den Umgang mit Informatik und Sicherheit geben.

Morgens bin ich jeweils die Erste, die anfängt, also schließe ich die Agentur und alle Büros auf und starte die Kaffeemaschine. Anschließend gehe ich an meinen Computer und starte diesen, damit ich Zugriff auf die Daten und das Internet habe. Am Morgen genieße ich die Ruhe, da kann ich alle Mails lesen und noch ein wenig im Internet surfen und lesen, was auf der Welt Interessantes geschieht. Allerdings muss ich in letzter Zeit oft studieren, ob eine bestimmte Mail jetzt wirklich von der Post oder einem Vertragspartner kommt oder nicht. Dann klicke ich zur Sicherheit jeweils auf den Anhang, dort steht ja, was ich wissen muss. Dabei hat mein Antivirenprogramm jetzt zweimal einen solchen Anhang gelöscht, was ich gar nicht verstanden habe, ich wollte doch nur nachsehen.

So gegen acht Uhr kommen dann die beiden Kollegen und die Chefin, und der Arbeitstag beginnt: Kunden bedienen, Post öffnen, Verträge schreiben, Policen einordnen oder auch mal Reklamationen bearbeiten – was alles so anfällt in einer Versicherungsagentur. Die Daten sind für mich zum Glück alle zugänglich, so kann ich auch der Chefin mal bei einem Vertrag unter die Arme greifen oder Arbeiten meiner Kollegen ordnen, die gerne alles einfach irgendwo speichern. Über Mittag gehen wir meist alle zusammen essen. Wir kennen da ein kleines Restaurant in der Nähe, das ist über Mittag zwar gut gefüllt, aber für uns halten sie immer einen Tisch frei. Das Büro schließen wir natürlich ab, die Systeme lassen wir laufen, damit wir nach der Pause nicht so viel Zeit verlieren, bis wir wieder arbeiten können.

Am Mittagstisch kann man schon auch mal was Privates bereden, aber auch aktuelle Vorgänge vom Vormittag, interessante Schadensfälle oder die neuesten Ideen unserer Kunden können wir hier ebenso besprechen. Das kann auch mal laut werden, aber meistens ist es einfach interessant – der Mittag ist immer schnell vorbei.

Am Nachmittag geht's wieder zurück in die Agentur. Während die beiden Kollegen dann öfter draußen bei den Kunden sind, bleibe ich in der Agentur für die Administration zuständig und erledige Telefonate oder bediene Kunden, die sich bei mir an den Tisch setzen, um mit mir ihre Sorgen oder Anliegen zu

besprechen. Erst letzthin hat mich ein potenzieller Kunde sehr genau über die Vorgänge auf unserer Agentur ausgefragt. Das war ein wenig eigenartig, aber ich möchte ja freundlich sein und habe so viele Auskünfte erteilt, wie ich konnte. So gegen 17 Uhr verlasse ich dann das Büro – abschließen tut in der Regel die Chefin, da sie meistens länger bleibt.

So weit ist eigentlich alles wie immer, wir sind organisiert, und ich bin auf meiner Stelle zufrieden. Nur nächste Woche, da müssen wir die Agentur für einen Tag schließen, weil unsere Zentrale uns alle in so eine Awareness-Schulung schicken will. Ich weiß zwar nicht, wozu das gut sein soll, bei uns ist ja noch nie etwas passiert – aber wenn es angeordnet ist, gehen wir hin und sehen, was wird. Vielleicht lässt sich ja noch etwas lernen.

1.1 Das Ziel dieses Buches

Laras Welt ist in Ordnung. Und für viele andere ist sie das auch, selbst wenn sie sich keine großen Gedanken über die Informatik machen, da sie diese als Instrument für ihre Arbeit nutzen und nicht als zentrales Thema um seinetwillen betrachten.

Oder denken Sie an IT, wenn Sie von einer Öl-Pipeline lesen? Und doch hat im Mai 2021 ein ebensolcher Angriff auf die IT-Systeme der größten amerikanischen Versorgungslinie dafür gesorgt, dass die Versorgungslinie selbst aus Sicherheitsgründen für mehrere Tage abgeschaltet werden musste. Und dies, obwohl durch diese Leitung mehr als 40 % der gesamten an der Ostküste verbrauchten Kraftstoffe laufen.

Oder denken Sie zuerst an IT, wenn Ihre Zeitung am Morgen nicht erscheint? So geschehen in Deutschland, als im April 2021 nach einem Hackerangriff zahlreiche Zeitung und Online-Portale der Madsack-Mediengruppe nicht mehr erreichbar waren oder Zeitungsteile über Tage nur in reduziertem Umfang produziert werden konnten.

Die Liste solcher und anderer Angriffe auf Unternehmen lässt sich mittlerweile täglich erweitern. Und die Folgen sind für die Unternehmen oft so gravierend, dass darüber nicht in den IT-Foren oder Security-Boards, sondern in der Tagesschau oder den Zeitungen berichtet wird. Die Angriffe zeigen überdies, wie eng die Verzahnung der eigentlichen Wertschöpfung von Unternehmen mit der Informatik und ihren Systemen mittlerweile ist – und wie manche »Laras aus Neustadt« immer noch auf unbekannte Mails klicken, sich an Telefonen ausfragen lassen oder Systeme unbeachtet laufen lassen.

Die Welt wird wegen eines neuen Buches nicht sicherer, doch mit wachsendem Bewusstsein für die Gefahren, denen unsere Daten und Systeme heute ausge-

setzt sind, lässt sich künftig wenigstens ein Teil solcher Angriffe erschweren oder verhindern.

Unser Buch soll dazu die notwendigen Anleitungen, Hilfestellungen, Erklärungen und praktischen Hinweise liefern, damit Ihnen das auch gelingen kann. Und Sie darüber hinaus auf die entsprechende Zertifizierung Ihrer Fähigkeiten als CompTIA-Security+-Techniker/-in gründlich vorbereiten.

Die folgenden Kapitel dieses Buches möchten Ihnen dazu das notwendige Wissen vermitteln und Ihnen eine Orientierung anbieten, damit Sie sich anschließend in den verschiedenen Themenbereichen der Netzwerk- und Systemsicherheit auskennen. So sind Sie auch in der Lage, sich von verschiedenen Seiten her mit der Thematik auseinanderzusetzen: von den Modellen wie IT-Grundschutz, ISO 27000 über die Bedrohungslage bis hin zur Implementation von Maßnahmen oder eines ganzen Security-Managementsystems!

Die Inhalte dieses Buches und eventuell auch ein dazugehöriges Seminar helfen Ihnen bei dem Verständnis der technischen Begriffe, der Funktionsweise von Sicherheitsmaßnahmen und den aktuellen Bedrohungen und einem praxistauglichen Vorgehen, um die Prüfung CompTIA Security+ bestehen zu können.

1.2 Die CompTIA Security+-Zertifizierung

CompTIA ist ein weltweiter Verband der Informationstechnologieindustrie. Der Verband wurde 1982 in den USA gegründet und zählt heute mehr als 20.000 Unternehmen und professionelle Branchenangehörige zu seinen Mitgliedern. CompTIA hat Mitglieder in mehr als 100 Ländern und liefert Technologiestandards in den Bereichen internetfähige Dienstleistungen, E-Commerce, herstellerunabhängige Zertifizierung, Kundenzufriedenheit, Public Policy sowie Ausbildung. Die Arbeit von CompTIA beruht auf einem kooperierenden Mitgliedsmodell – das heißt, Hersteller, Dienstleister und Beschäftigte der IT-Industrie arbeiten bei der Formulierung und Umsetzung konkreter Ziele zusammen.

Insbesondere im Bereich der IT-Zertifizierung hat sich CompTIA weltweit einen anerkannten Ruf erworben und ist heute der größte herstellerunabhängige Anbieter von Zertifizierungen im Bereich der Informationstechnologie. Die Basis für die anerkannte Güte der CompTIA-Zertifikate ist nicht zuletzt deren gemeinschaftliche Entwicklung durch IT-Fachkräfte und Mitgliedsunternehmen. Da ein großes Problem der IT-Branche der Wildwuchs zahlreicher Fort- und Weiterbildungsmaßnahmen ist, bietet CompTIA insbesondere im Rahmen der technischen Grundausbildung hochwertige Zertifikate an, die Privatpersonen wie Unternehmen die Orientierung auf dem unübersichtlichen Fortbildungsmarkt erleichtern sollen.

Das erklärte Ziel von CompTIA ist die Etablierung von technischen und fachlichen, aber auch ethischen und professionellen Qualitätsstandards in der IT-Industrie. Indem Unternehmen wie Cisco, Hewlett-Packard, IBM, Intel, Microsoft und Ricoh die Entwicklung der Zertifikate von CompTIA finanziell und mit ihrem Know-how unterstützen, gewinnen sie gleichzeitig Anhaltspunkte über die Fachkompetenz und ein sicheres Anforderungsprofil für die Auswahl von Mitarbeitenden.

Weltweit haben mehr als eine Million Menschen CompTIA-Zertifikate in Systemtechnik, Netzwerktechnologie, Serverbetreuung und anderen Gebieten erworben.

Die CompTIA Security+-Zertifizierung wendet sich an Techniker mit eigener Berufserfahrung im Informatikbereich und bescheinigt dem Träger eine breite Kenntnis auf dem Gebiet der Sicherheitstechnologie. Das bestandene Examen bedeutet, dass der Geprüfte über ausreichend Wissen verfügt, um die Bedrohungslage zu verstehen und eine Reihe von Maßnahmen zu konfigurieren bzw. in Betrieb zu nehmen. Im Rahmen der Zertifizierung werden zahlreiche herstellerunabhängige Technologien behandelt. Die CompTIA Security+-Prüfung eignet sich sehr gut als Vorbereitung auf die IT-Zertifikate diverser, im Security-Sektor aktiver Hersteller.

Damit die Zertifizierung am Markt erfolgreich bleibt, wird die Prüfung durch die CompTIA regelmäßig aktualisiert und an die aktuellen Anforderungen angepasst, und so liegt mittlerweile die vierte Version von CompTIA Security+ vor. Die Inhalte der Zertifizierung werden anschließend in Lernzieldokumenten auf der Website von CompTIA unter `www.comptia.org` veröffentlicht (sogenannte »Exam Objectives«).

Die CompTIA Security+-Zertifizierung teilt sich in mehrere Fachgebiete, im CompTIA-Sprachgebrauch »Domains« genannt. In der aktuellen Fassung der Prüfung (SY0-601) lauten diese Themen wie folgt:

Domain 1	Bedrohungen, Attacken und Schwachstellen
Domain 2	Architektur und Design
Domain 3	Implementation
Domain 4	Betrieb und Incident Response
Domain 5	Governance, Risiko-Management und Compliance

Entsprechend erhalten Sie in diesem Handbuch zur Sicherheit alle genannten Themen und ihre Zusammenhänge ausführlich erklärt und erlernen so zugleich das für die Zertifizierung notwendige Wissen. Im Zentrum steht dabei weniger die Auflistung aller möglichen und unmöglichen Abkürzungen aus diesem Bereich, sondern die Schaffung des Verständnisses für die Thematik Sicherheit. Für die Abkürzungen finden Sie zudem ein Abkürzungsverzeichnis im Anhang dieses Buches, ebenso wie eine Zuordnung der einzelnen Lernziele zu den Inhalten des Buches.

1.3 Voraussetzungen für CompTIA Security+

Gemäß der Website von CompTIA (`www.comptia.org`) sind die empfohlenen Voraussetzungen für das Bestehen der Security-Prüfung die CompTIA Network+-Zertifizierung sowie zwei Jahre Erfahrung im Netzwerkbereich mit Schwerpunkt Sicherheit.

Diesen Empfehlungen stimmen die Autoren natürlich zu. Dieses Buch kann Ihnen nicht die praktische Erfahrung vermitteln, die im Bereich Netzwerktechnik nötig ist, um erfolgreich zu sein. Wenn Sie sich also auf die Zertifizierung vorbereiten möchten, lesen Sie dieses Buch, aber installieren Sie auch selbst ein Netzwerk, befassen Sie sich regelmäßig mit Sicherheitsthemen, gehen Sie in ein Training oder bauen Sie mit Kollegen eine Umgebung auf, die dafür geeignet ist, und üben Sie sich praktisch in der Erkennung von Bedrohungen, der Anwendung von Sicherheitsmaßnahmen und -konzepten.

Für weitere Informationen begeben Sie sich bitte auf die Website von CompTIA unter `www.comptia.org/de`. Details zur Prüfung finden Sie zudem in Kapitel 21, »Die CompTIA Security+-Prüfung«.

Wenn Sie den an dieser Stelle von CompTIA zur Verfügung gestellten Code »Kabera10« nutzen, so erhalten Sie auf den Kauf eines CompTIA-Prüfungs-Vouchers 10 % Rabatt.

1.4 Persönliches

Wer sich zum ersten Mal mit der Thematik Informatiksicherheit befasst, wird vor allem eins feststellen: Es wimmelt nur so von Fremdwörtern und Fachbegriffen. Von Antispam über Phishing bis zum Zombie ist alles vertreten, was das Alphabet zu bieten hat.

Als Autoren staunen wir manchmal selbst über die Vielfalt an Kreationen, die hier geschaffen werden – auch wir mussten nachdenken, als wir zum ersten Mal über »Whaling« gelesen haben ... und längst nicht alle Begriffe verfügen über den gleichen Tiefsinn oder fachlichen Rückhalt.

Ein Buch zur Informatiksicherheit zu verfassen, ist daher eine Gratwanderung zwischen der notwendigen Vermittlung von Fachwissen und der Zurückhaltung gegen ein Überborden von Pseudofachbegriffen und (vorwiegend) Anglizismen, die mehr vorgeben, als sie wirklich bedeuten.

Wir haben uns daher beim Schreiben bemüht, Ihnen einen Überblick zu ermöglichen, sich mit den zentralen Themen vertraut zu machen und vor allem die Thematik zu verstehen, aber nicht schlicht Begriffe auswendig zu lernen – obwohl sich das prüfungstechnisch nicht ganz vermeiden lässt.

Es ist unsere feste Hoffnung, dass wir Sie mit diesem Buch für die Thematik der Informationssicherheit über die reine Prüfung hinaus sensibilisieren können, Ihnen Hilfen an die Hand geben und Sie ausrüsten für einen sinnvollen und sicheren Umgang mit Informationen und Informatikmitteln in Ihrem Umfeld.

Zu den Autoren selbst:

Mathias Gut, Master of Advanced Studies ZFH in Business Analysis und Dipl. Informatiker, ist Information- und Cyber-Security-Experte. Er ist in verschiedenen Bereichen von Sicherheitsfragen ausgebildet und zertifiziert, unter anderem als zertifizierter OSSTMM Professional Security Tester (OPST), zertifizierter IT-Grundschutz-Praktiker, zertifizierter ICO ISMS 27001:2013 Foundation, CompTIA Advanced Security Practitioner (CASP), CompTIA Security+, CompTIA Network+, CompTIA Linux+ und hat zusätzlich ein abgeschlossenes Studium in CAS Information Security & Risk Management der Fachhochschule Nordwestschweiz. Er arbeitet täglich mit Fragen der Sicherheit und unterrichtet zudem als Dozent im Bereich der Informationstechnik mit Schwerpunkt IT-Sicherheit in der höheren beruflichen Bildung. Als impulsgebender Entwickler und Mitdozent des von der HWZ verliehenen CAS Cyber Security Expert übernimmt er eine aktive Rolle in der Weiterbildungslandschaft. Als Initiator und Lead-Programmierer des Open Projects »Free & Open Cyber-Security Analysis Framework« setzt er sich in seiner Freizeit für quelloffene Software und freie Analysemethoden ein (`www.freecybersecurity.org`).

Markus Kammermann, ursprünglich Theologe, später weitere Berufsbildungen zum IT-Projektleiter und Ausbilder, SCRUM Master, CompTIA Security+ und weitere Zertifizierungen, ist Autor mehrerer Fachbücher aus der CompTIA-Zertifizierungsreihe bei MITP. Allen voran des bereits in 7. Auflage erschienenen Grundlagenwerks »CompTIA Network+« sowie des in 5. Auflage verlegten Studienwerks »CompTIA A+«. Er arbeitet seit vielen Jahren als technischer Berater, Dozent und Referent in verschiedenen Ländern und ist in seiner Seele ein »Erklärer«, der nach wie vor selbst konzipiert, vernetzt und installiert und somit die Sicherheit in der IT tagtäglich erlebt, gerade wenn sie nicht funktioniert. Als Dozent in der höheren beruflichen Bildung und Autor ist es ihm wichtig, nicht nur Sachverhalte darzulegen, sondern sie verständlich zu machen, denn Lernen lebt nicht vom Hören, sondern vom Verstehen und Befähigtwerden.

Wir danken Frau Rechtsanwältin Chantal Lutz (Associate, CIPP/E), Herrn Rechtsanwalt Christian Mitscherlich (Partner) und Herrn Christoph Domke (Junior Associate) von der Kanzlei Domenig & Partner Rechtsanwälte AG für ihren wertvollen Beitrag zu den Themen Datenschutz und Cybercrime. Ihre Kanzlei Domenig & Partner Rechtsanwälte AG aus Bern besteht aus führenden Datenschutzexperten der Schweiz, die an der Redaktion des neuen schweizerischen Datenschutzgesetzes mitgewirkt haben. Private Unternehmen und die öffentliche Hand zählen bei der Bewältigung der datenschutzrechtlichen Herausforderungen auf die Hilfe des Datenschutzrechtsteams von der Domenig & Partner Rechtsanwälte AG.

Anlässlich der anwaltlichen Beratung beschäftigen sich die Autoren täglich mit der Umsetzung von Vorgaben der DSGVO und des neuen schweizerischen Datenschutzgesetzes. Diese umfangreiche Praxiserfahrung ließen die Autoren bei der Redaktion des neuen Kapitels 4, »Rechtliche Grundlagen« der vierten Auflage dieser Publikation einfließen.

Bedanken möchten wir uns an der Stelle auch bei Markus a Campo, der an der ersten Auflage aktiv mitgearbeitet und damit etliche Vorarbeit vor allem zur 2. Auflage beigetragen hat. Er arbeitet als Berater, Autor und Schulungsreferent mit dem Schwerpunkt IT-Sicherheit. Er ist von der IHK Aachen öffentlich bestellter und vereidigter Experte im Bereich IT-Sicherheit.

Bedanken möchten wir uns an dieser Stelle zudem ausdrücklich bei den Herstellern und ihren Kommunikationsabteilungen, die uns mit Bildmaterial und Unterlagen unterstützt haben.

Ebenso möchten wir uns an dieser Stelle beim mitp-Verlag bedanken und persönlich bei Katja Völpel – ja, wir haben wieder einen Titel zusammen publiziert, und das ist erfreulich.

Wir wünschen Ihnen viele spannende Stunden, ob in einem E-Book am Tablet bzw. PC oder vor Ihrem Papierexemplar.

Stichwortverzeichnis

2,4-GHz-ISM-Band 457
3DES 110
5-GHz-ISM-Band 457
802.11ac 456
802.11b 454
802.11g 454
802.11i 468
802.11n 455
802.11p 459
802.11s. 459
802.1x 436, 470

A

AAA-Protokoll 439
Absichtserklärung 359
Access Control List 136, 146
Access Point
  Captive Portal 229
  Evil Twin 228
  Rogue 228
Ad hoc 464
Ad-hoc-Netzwerk 459
Administrative Richtlinie 58
Advanced Threat 278
Adversary tactics, techniques and procedures (TTP) 218
Adware 180, 181, 278
AES 111
AH 442
AIRO 499
Akteur 421
  staatlicher 424
Amplification-Attack 411
AMSI 272
Annual Loss Expectancy 578
Antivirus-Evasion-Methode 268
API 234
App 302
  Whitelist 305
Application Gateway 521, 523
Application Level Gateway 515
Application-DDoS 411
APT 191, 193, 216
Arbitrary Code Execution 207
Archivierung 316, 345
ARP 503
  NDP 503
Artificial Intelligence (AI) 234, 272
ASLR 208, 280, 282
ASP 388
Asset Tracking 302
Asymmetrische Verschlüsselung 112, 120
Attack Surface Reduction (ASR) 272
Attacke
  Advanced Persistent Threat 193
  Carbanak 217
  DNS-Tunneling 227
  HID-Angriff 221
  Kaltstartattacke 221
  MMS-Phishing 192
  Pass-the-Hash 213, 214, 220
  Pharming 192
  Phishing 192
  Rootkit 419
  SMS-Phishing 192
  Zero hour 192
Aufbewahrung 316
Aufbewahrungspflicht 346
Aufgabenteilung 324
Aufnahmemöglichkeit
  mobiles Gerät 310
Ausfallszenario 577
Authentifizierung 138
Authentifizierungsmethode 137
Autorisierung 136
Awareness 271, 324, 333

B

BaaS 388
Backdoor 193, 214, 222, 224, 419
Badge 158, 160, 232
BAD-USB-Angriff 222
Baselinemanagement 486
Baseline-Messung 242
BASH 211
Bastion Host 521

Bauliche Maßnahme 157
BCM 564
BCMS 564
Bcrypt 120
Bell La Padula 145
Benutzerverwaltung 58
Beweismittel 553
Bildschirmsperre 301
  Notebook 299
Biometrie 140
Biometrisches Erkennungssystem 161
Birthday-Attacke 537
Black Hat 423
Black-Box-Test 543
Blockverschlüsseler 107
Blowfish 111
Bluejacking 477
Bluesnarfing 477
Bluetooth 476
Bogus Access Point 414
Bogus DHCP-Server 415
Bombe
  logische 193
Boot-Virus 186
Bösartiges USB-Kabel 222
Bot 450
Botnet 237, 412, 425, 450
Brandklasse 166
Brandschutz 165
Bring Your Own Device 306
Broadcast 365
Brute Force 400
BSI 50, 52
  Bausteine 53
  Schichtenmodell 53
Buffer Overflow 207, 208
Bug-Bounty 427
Business Continuity Management 347
BYOD 306

C

CA 121, 126, 128
Cache-Poisoning 382
CBC 107, 124
CCMP 468, 469
CCPA 323
CEO Fraud 332
CERT 396
Certificate Authority 121, 126, 128
CFB 108
Chain of Trust 128
CHAP 150
Chassis Intrusion Detection 249
Choose Your Own Device 306
CIA 45, 103
CIFS 387
Cipher text only 123
Circuit Level-Firewall 522
Clean Desk Policy 319
Cleanup 543
Clickjacking 410
Cloud 419
  Public-Cloud-Dienste 303
  Sicherheit 388
Cloud Computing 255
  IaaS 388
  PaaS 388
  SaaS 388
Cloud Security Alliance 391
Cluster 574
Clustering 573
  HA-Cluster 573
  NLB 574
  SMP 573
CO_2 166
Codesignierungs-Zertifikat 130
Cold Site 584
Command Shell (CMD) 211, 218
Command-and-Control 425, 450, 529
Command-Injection 405
Common Criteria 48, 251
Common Name 129
Compliance 320
CompTIA Security+- 26
Cookie-Diebstahl 418
Cookie-Manipulation 405
COOP 587
COPE 306
Corporate Owned Personally Enabled 306
Credential Guard 221
Credential harvesting 200
Credential-Management 304
Crimeware 183
CRL 131, 140
Cross Site Scripting 403
Cryptomalware 197
Cryptomining 197
CSA 391
CSF 50
CSP 105, 403
CSR 126
CTR 108
cuckoo 538
curl 538
CVE 209, 547, 551
CVSS 209, 547

Cyberkriminalität 179, 425
Cyberkriminelle 179
Cyber-War 422
CYOD 306

D

DAC *siehe* Zugriffssteuerung
Darknet 209, 425
Darkweb 195, 209
Data Execution Prevention 281
Data Loss Prevention 318
Data-at-rest 122
Data-Carving 557
Data-in-transit 122
Data-in-use 122
Datenhaltung 316
Datenschutz 66
Datenschutzgesetz 320
    Datensicherung 346
Datensicherung 274, 344, 345, 348, 352
Datensicherungskonzept 348
Datensicherungsmedium 345
DCS 255
DDoS 237
Deauthentication 230, 231
Dedizierte Firewall 513
Deep Fake 235
Deep Learning 235
Deep Packet Inspection 305
Degaussing 357
Denial of Service 194, 207, 231, 397, 410, 450
DEP 208, 280, 281
DES 110
DevOps 289
DH 114
DH-Gruppen 114
Diebstahlsicherung 248
Dienstleistungsrahmenvertrag 359
Differenziell *siehe* Datensicherung
Diffie-Hellman 114
Diffusion 106
Digitale Signatur 120
Directory-Traversal 401
Disassoziation 231
Disaster Recovery 58, 352, 575
Disk
    Full Disk Encryption 250
    Opal 250
    SED 250
Disposal-Management 89, 357
Distributed Denial of Service 412
DKIM 339
DLL-Injection 208
DLP 318
DMARC 273, 339
DMZ 512, 516
DNS 382, 516
dnsenum 538
DNS-Flooding 205
DNS-Poisoning 205
DNS-Spoofing 205
Domain 253
Domain Hijacking 410
Domänenrichtlinie 245
Doxing 206
Dragonblood 229
Drehschleuse 162
Drive-by-Angriff 408
Drive-by-Pharming 205
Drohnen 233
DSGVO 75, 82, 320
Dual-homed Firewall 514
Due-Diligence 322
Dumpster Diving 328
Duplexing 572

E

EAP 471
EAP-TLS 437
Eavesdropping 449
ECB 107
ECC 115
EDR 269
EICAR 276
Einbruchsschutz 164
EIP 208
Elektrostatische Entladung 169
ElGamal 115
E-Mail-Protokolle 383
E-Mail-Sicherheit 333
Embedded-System 290
EMP 175
Endpoint-Protection 269
Energieversorgung 170
Enigma 104
Entladung
    elektrostatische 169
Erkennungssystem
    biometrisches 161
Error Handling 290
    SEH 290
ESD 169
ESD-Strip 169
ESP 443
Evil Twin 225, 228
Evil-Maid 212

Exploit 207, 542
Extranet 519

F

False-Negative 546
False-Positive 542, 546
FCAPS 482
FDE 250, 299
Fehler
  kritischer 262
  sicherheitskritischer 261
File Inclusion
  LFI 401
  RFI 401
Fileless Malware 198
Fingerabdrucksensor 300
Fingerprint 141
Fingerprinting 541
FINMA 50
Firewall 517
  Circuit Level 522
  dedizierte 513
  Dual-homed 514
  Hardware- 513
  Paketfilter 520
  Personal 513, 517
  Software-Firewall 252
  Stateful Packet Inspection 520
  Typen 515
  UTM 525
FireWire-Hack 221
Firmware 215, 222, 231, 247, 248, 251, 257, 259, 475
FISMA 322
Fleeceware 181
FOMO 183
Footprinting 539
Forensik 551
FORM-Field 405
FTP 381
Full Device Encryption 299
Fuzzing 550

G

Gangerkennung 141
GCM 108
Generationenprinzip *siehe* Datensicherung
Geo-Tagging 305
Gerätename 478
Gerätesperre 300
Geschlossenes System 285
Gesichtserkennung 140
Google-Hacking 328
Governance 321
GPDR 82
GPS-Tracker 299
Gray Hat 424
Grayware 180
Gruppenrichtlinie 245

H

H2M-Schnittstelle 256
Hackertatbestand 78
Hacktivist 425
Hardware-Firewall 513
Hardware-Sicherheitsmodul 251
Hardwarevirtualisierung 253
Hash 150
Hash-Wert 117
Header 557
Hierarchische PKI 126
HIPAA 322, 347
HIPS 269, 270
HMAC 119
Hoax 198
Hochwasserschutz 165
Höhere Gewalt 575
Honeynet 525
Honeypot 525
Hot Site 58, 584
Hotfix 263, 402, 546
HOTP 139
hping3 542
HSM 130, 251
HSTS 291
HTTP 383, 516
Hybrid Cloud 389
Hybride Verschlüsselung 121
Hybrid-RAID 569
Hypervisor 253

I

IaaS 388, 420
ICS-Server 256
Identifizierung 137
Identität 135
IDS 525, 526, 527
IEEE 802.11 454
ifconfig 500
IGMP 379
IKE 445
Impersonation 329
Implementierung 376
Implicit Deny 136
Incident Response 552
Incident Response-Team 585

Incident-Management 275
Industrie 4.0 254
Influence Campaigns 332
Information Gathering 213, 327
Information Security Management System 57
Informationsklasse 314
Informationsrichtlinie 58
Infrastrukturnetzwerk 460
Inkrementell *siehe* Datensicherung
Integer Overflow 208
Integrität 44
Internet of Things 235, 256
Intranet 519
Intrusion Detection 525
Intrusion Prevention 525
Intrusion Prevention System 527
Invoice scams 332
IoC 213, 288
IoT 235, 256, 261, 290
ipconfig 500
ip-Kommando 501
IP-Protokoll 376
IPS 527
IPsec 441, 444
IPv6 379
Iris-Scan 140
ISA 359
ISMS 57, 575
ISO/IEC 27001 50
IT-Grundschutz 54
ITSEC 47
IV-Attacke 467

J

Jamming-Angriff 231
Job-Rotation 324

K

Kensington 248
Kerberos 149
Kerckhoff-Prinzip 123
Kernprotokoll 376
Keycard 159, 232
Keylogger 211, 408
Key-Stretching 105
Klassifizierung
  Informationen 314
  zur Datenhaltung 317
Klimaanlage 175
Known plain text 123
Kollision 401
Konfigurationsmanagement 242
Konfusion 106
Kopplung *siehe* Bluetooth
KRACK-Attacke 229
Kriminalität
  organisierte 425
Kriminelle Aktivitäten 576
Kritischer Fehler 262
Kryptografie 104
Krypto-Malware 197
Künstliche Intelligenz (KI) 234, 272

L

L2TP 441
Länderfilter 280
LANMAN 120
Lastwert 486
Lateral Movement 214, 220
LDAP 387
LDAP-Injection 404
Least Privileges 149
Legacy 259
Leistungsbeschreibung 358
Leistungsüberwachung 487
Letter of Intent 359
Lifecycle-Management 289
Living-off-the-Land-Hacking 211, 218
Loadbalancing 573
Lockout 300
Logdaten 603
Logfile-Analyse 604
Logische Bombe 193
LoMAC 145
Löschen 357
LSASS 220
LSO 408
Luftfeuchtigkeit 176

M

M2M 256
MAC *siehe* Zugriffssteuerung
MAC-Cloning 413, 475
MAC-Flooding 415
MAC-Spoofing 413, 475
Mail Spoofing 339
Mail-Gateway 342
Makrovirus 187, 272
Malvertising 403
Malware 183
  Adware 180
  Antispyware 182
  Arbeitsweise 186
  Crimeware 183
  Grayware 180

Spam 180
Spyware 180
Symptome einer Infektion 185
Malware Dropper 192, 198, 210, 214, 220, 268
Malware Injector 210
Malwaretising 210
Man in the Browser 410
Man in the Middle 414, 416, 449
Man Trap 162
Managed Objects 481
Management Information Base 482
Mandatory vacations 324
Mannschleuse 162
Maßnahme
bauliche 157
Maus 287
MD4 118
MD5 118
Memory Leak 290
Memory of Understanding 359
Menschliches Versagen 575
Metasploit Framework 550
Mimikatz 213, 221
MIMO 455
Mining Rig 197
Mirror 567
MITRE ATT&CK® 218
Modus 1 *siehe* Bluetooth
MOU 359
MouseJack 224
MRTG 495
MTO 355, 579
MTR 505
Multifaktorauthentifizierung 142
Multi-Level-Security 145
MU-MIMO 457

N

NAC 367
Nagios 497
NAS 439
NAT 366
DNAT 366
NAPT 366
PAT 366
SNAT 366
SUA 366
Negative Rules 515
Nessus 538
NetBIOS 387
netcat 538
netstat 506
Network Access Server 439, 471
Netzwerkmonitor 490, 491
Netzwerk-Sniffer 549
Netzwerküberwachung 490
NFC 231
Nicht sichtbar *siehe* Bluetooth
Nicht-Leugbarkeit 152
NIDS 526
NIPS 269, 526
NIST 50
Non-Disclosure Agreement 537, 539
Non-Repudiation 151
NOP 208
NoSQL-Datenbanksystem 291
Notebook
Bildschirmsperre 299
Notfallplan 580
Notfallvorsorge 58, 565
Notstromaggregat 172
nslookup 505
NTLM 120, 151

O

OCSP 127
OFB 109
Öffentlicher Schlüssel 113
OID 128
OLA 358
One-Time-Pad 106
Online-Backup 355
Open Framework Certificate Transparency 287
Operational technology (OT) 236, 237
Organisierte Kriminalität 425
OSINT 206, 328, 332
Outsourcing 59
OWASP 290, 291

P

PaaS 388
Paketfilter 515, 519
Paketfilter-Firewall 520
PAP 150
Pass-the-Hash 213, 214, 220
Passwort
Regeln 138, 152
Passwort Guessing 399
Passwort-Cracker 213, 548
Passwort-Guesser 548
Passwort-Spraying 548
Patch 262
Patch-Management 264
PBKDF2 120

PCI-DSS 323, 498
PEAP 437
PEAP-EAP-TLS 438
Penetration Testing 535
Penetrationstest 212, 536
  Blue Team 536
  Purple Team 536
  Red Team 536
  White Team 536
Perfect Forward Secrecy 116
Persistence 214
Personal Firewall 513, 517
Personendaten 70
PFS 116, 121
PGP 335
Pharming 205
Phishing 81, 199, 406
Phishing-Site 271
PII 320
PIN-Code 297
Ping 502
Ping of Death 411
ping6 502
Pivoting 213
Pixie Dust 231
PKI 125, 131
  hierarchische 126, 132
Playbook 275, 585
PLC 256
Portnummer 380
Portscanner 541
Positive Rules 515
Post Exploitation 213
Potentially unwanted programs 181
PowerShell 211, 218, 272
PPP 379
PPTP 440
Prepending 332
Pretexting 328
Privacy by default 77
Privacy by design 77
Private Cloud 389
Privater Schlüssel 113
Privilege Escalation 212, 213
Problemkategorie 262
Proxy 522
PSK 446
Public Cloud 389
Public-Cloud-Dienst 303
Pufferüberlauf 398
Punkt-zu-Punkt-Verbindung 432
Python 211

Q

Quantenkryptografie 116
Quarantänebereich *siehe* NAC

R

RA 126
Race-Condition 399
RADIUS 438, 440, 470, 471
RAID 566
RAID 0 567
RAID 1 567
RAID 10 569
RAID 5 568
RAID 50/51 570
RAID-Level 566
Rainbow-Tabelle 401, 548
Ransomware 188, 195, 280
Rasperry Pi 234
RAS-System 436
RAT 211, 212
RBAC *siehe* Zugriffssteuerung
RC4 112
RDR 269
Reconnaissance 327
Recovery-Agent 131
Redundanz 583
Refactoring 407
Registration Authority 126
Registrierung 126
Release-Note 547
Remote Sanitation 299
Remote Wipe 299, 301
Remote-Access 431
Remote-Access-VPN *siehe* VPN
Remote-Zugriff 431
Replay-Angriff 108, 226, 384, 416
  Session-Replay-Angriff 416
Reputationslösung 270
Resilienz 565
Resource Exhaustion Attack 207
Retention Policy 588
Retina-Scan 140
RFC 535
RFID 231
Richtlinie
  administrative 58
  Informationsrichtlinien 58
  Systemsicherheitsrichtlinien 58
RIPEMD 119
RMON 484
Rogue Access Point 228, 476
Rollen 137
Rollenbasierte Zugriffskontrolle 146

Rollups 263
Rootkit 192, 419
Root-Zertifikat 127
ROP 282
RPO 355, 578
RSA 114
Rules of Engagement 539
Runbook 275

S

S/MIME 334, 335
SA 442, 445, 446
SaaS 388, 419
Safe 164
Safe Erase 89
Salt 401
SAML 137
Sandbox 524
Sanitation 301
SAN-Zertifikat 129
SAO 499
SCADA 255, 257
Scalper 182
scanless 538
Scarcity 183
Schadensausmaß 581
Schadsoftware 180
Schatten-IT 426
Schleuse 162
Schließsystem 158, 160
Schlüssel 158
  öffentlicher 113
  privater 113
Schlüsselbund 337
Schlüsselverwaltung 304
Schutzbedarf 320
Schutzbedarfsfeststellung 54
Schwache Verschlüsselung 124
Schwachstellen-Scanner 544
SCP 381
Scraping 182
Screenlock 301
Script-Kiddies 426
Secure Header 291
Security Operations Center 533, 547
Security-Scanner 544
Segretation of Duty 324
SEHOP 280, 282, 290
Sender Policy Framework 201
Serverraum 176
Service Pack 263
Session-Hijacking 417
SHA 118
Shimming 407
Shoulder surfing 330
Sicherheit
  organisatorische 46
  physische 46
  technische 46
Sicherheitskritischer Fehler 261
Sicherheitsrichtlinie 244
Sicherheitsvorlage 246
Sicherungsverfahren *siehe* Datensicherung
Sideloading 278, 305
SIEM 288, 498
Signatur
  digitale 120
SIPS 449
Site-to-Site *siehe* VPN
Skimming 81, 233
SLA 357
  Fehlerraten 358
  Leistung 358
  Reaktionsbereitschaft 358
  Sanktionen 358
  Verfügbarkeit 358
SLIP 379
Smishing 204
SMON 484
SMTP Relay 338
Smurf 411
SN1PER 538
Snapshot 353
Sniffing 225
SNMP 383, 484
SOAR 276, 499
SOC 499, 533, 547
Social Engineering 313, 326, 333
Social Media 342
Software Maintenance 261
Software-Firewall 252
Something you know 138
SOX 347
Spam 180, 340, 409
Spear Phishing 204
SPF 201, 273, 339
Spim 204, 409
Spit 409
Spoofing 225, 413, 449
Spyware 180, 181, 211, 278
SQL-Injection 404
SRTP 449
SSH 381, 447, 516
SSID 463
SSL 384, 447
SSL Stripping 223, 285

SSL-Zertifikat 128
SSO 137
Staatlicher Akteur 424
Stack 398
STAR-Zertifizierung 391
Stateful Packet Inspection Firewall 515, 520
Steganografie 420
Stimmenerkennung 141
Stripe 568
Stromverbrauch 176
Stromverschlüsseler 108
Stromverschlüsselung 109
Stromversorgung 170
Stuxnet 217
SUA 366, 367
Subnettierung 365
Subnetzmaske 364
Supply Chain 59, 423
Supply-Chain-Attacke 217
Switch-Überlastung 415
SY0-301 608
Symmetrische Verschlüsselung 109, 120
SYN-Flooding 410
System
  geschlossenes 285
Systemhärtung 246
Systemintegrität 252
Systemsicherheitsrichtlinie 58

T

TACACS 439
TACACS+ 439
Tailgating 331
Tastatur 287
TCG 250
TCP 377
TCP-Hijacking 414
tcpreplay 526
TCSEC 47
Technisches Versagen 575
Telnet 381
Terminalverbindung 381
TFTP 381
theHarvester 538
Threat Intelligence 288
Timeline 557
Time-of-Check-to-Time-of-Use (TOCTTOU) 399
TKIP 468
TLS 384
Tokenization 323
TOM 75
TOR 195
TOTP 139
TPM 250, 274
Traceroute 504
tracert 504
tracert-6 504
Transitive Trust 305
Transitiver Zugriff 406
Transport-Modus 443
Transportverschlüsselung 380
Treibermanipulation 407
Triple-A 439
Trust-Center 121, 124, 128
Trusted Platform Module 250
Trust-Modell 125
Tunnel-Modus 443
Twofish 112
Typo squatting 409

U

UAC 213
UAV 233
Überwachung 483
UDP 378
UEFI-BIOS 274
Unified Threat Management 512, 528
Update 263
Upgrade 264
UPS 170
URL-Hijacking 409
URL-Manipulation 405
URL-Redirection 410
USB-Kabel
  bösartiges 222
User Behaviour Analytics 498
USV 170, 171
  Leistung 171
UTM 512, 528
UTM-Firewall 525

V

VBA 187, 211
Vektor 423
Venen-Scan 141
Venen-Scanner 141
Verfügbarkeit 44
Verschlüsselung
  asymmetrische 112, 120
  hybride 121
  schwache 124
  symmetrische 109, 120
Vertraulichkeit 44
Videoüberwachung 163
Virenbekämpfung 266

Virenschutzkonzept 274
Virenverantwortlicher 275
Virtualisierung 364
Virus 184, 273
  Botnet 190
  Makroviren 187
  Trojanisches Pferd 189
  Unterarten 186
  Würmer 194
Vishing 203
VLAN 368
VoIP 449
Vollbackup *siehe* Datensicherung
Voraussetzung
  für Zertifizierungen 31
VPN 431
VPN-Konzentrator 435
VPN-Lösung 303

W

Wachpersonal 159
WAF 292
WAP 472
War Chalking 453
War Driving 453
War Flying 233, 453
Watering Hole 210
Webantivirus 271
Web-Spoofing 415
WEP 466
Whaling 205
Whistleblowing 425
White Hat 423
White-Box-Test 543
Whitelisting 269, 279
Widerstandsfähigkeit 566
Wildcard-SSL-Zertifikat 129
Wiping-Verfahren 300
WIPS 476
Wireshark 492
Wirtschaftsspionage 425
WLAN
  Analyse 495
  Aufbau 461
  CB 461
  DFS 456
  ESS 460
  Heatmap 463
  LWAPP 460
  MAC-Filter 464
  Outdoor 455
  Stör- und Dämpfungsfelder 462
  TPC 456
  Verschlüsselung 464
Wörterbuch-Angriff 548
WPA 469
WPA2 469
  Enterprise 469
  PSK 469
WPA3 469
WPS 230
Wrapper 278

X

X.509 125, 127, 446
XaaS 388
Xmas-Attacke 411
XML-Injection 405
XSRF 200, 416
XSS 200, 291, 403
  Reflective XSS 403
  Stored XSS 403
XTACACS 439

Z

Zeitsteuerung *siehe* Rollen
Zero-Day Exploit 207, 217, 342, 396, 424
Zero-Knowledge 60
Zertifikat 126
  Revocation 131
  SSL 128
  zurückziehen 131
Zugriff
  transitiver 406
Zugriffskontrolle
  rollenbasierte 146
Zugriffsliste 136
Zugriffssteuerung 144
Zutrittsregelung 158