Inhaltsverzeichnis

1 Sichtweisen auf die Cyber-Sicherheit im Cyber-Raum 1
1.1 Einleitung 1
1.2 Cyber-Sicherheitsherausforderungen im Cyber-Raum 5
1.2.1 Cyber-Sicherheitsherausforderung „Zu viele Schwachstellen in Software“ 6
1.2.2 Cyber-Sicherheitsherausforderung „Ungenügender Schutz vor zunehmender intelligenter Malware“ 7
1.2.3 Cyber-Sicherheitsherausforderung „Keine Lösungen für Identifikation und Authentifikation für den gesamten Cyber-Raum“ 9
1.2.4 Cyber-Sicherheitsherausforderung „Unsichere Webseiten im Internet“ 9
1.2.5 Cyber-Sicherheitsherausforderung „Gefahren durch die Nutzung mobiler Geräte“ 10
1.2.6 Cyber-Sicherheitsherausforderung „Mehr E-Mail – mehr Risiko“ 11
1.2.7 Cyber-Sicherheitsherausforderung „Unsichere IoT-Geräte und -Plattformen“ 12
1.2.8 Cyber-Sicherheitsherausforderung „Internetnutzer haben zu wenig Medien-Kompetenz im Cyber-Raum“ 14
1.2.9 Cyber-Sicherheitsherausforderung „Manipulierte IT und IT-Sicherheitstechnologien“ 15
1.2.10 Cyber-Sicherheitsherausforderung „Geschäftsmodell: Bezahlen mit persönlichen Daten“ 16
1.2.11 Cyber-Sicherheitsherausforderung „Fake News“ und weitere unerwünschte Inhalte 17
1.3 Problematische Rahmenbedingungen im Cyber-Raum 18
1.4 Gesellschaftliche Herausforderungen im Cyber-Raum 19
1.4.1 Privatsphäre und Datenschutz 19
1.4.2 Selbstbestimmung und Autonomie 21
1.4.3 Wirtschaftsspionage 22
1.4.4 Cyberwar 23
1.5 Wechseln vom Paradigmen im Cyber-Raum 24

Bibliografische Informationen
http://d-nb.info/1244543527

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

1.5.1 Paradigmenwechsel „Verantwortung versus Gleichgültigkeit“ ... 25
1.5.2 Paradigmenwechsel „Proaktive versus reaktive Cyber-Sicherheitslösungen“ ... 25
1.5.3 Paradigmenwechsel „Objekt-Sicherheit versus Perimeter-Sicherheit“ ... 26
1.5.4 Paradigmenwechsel „Cloud-Service versus Lokal-IT“ ... 27
1.5.5 Paradigmenwechsel „Dezentrale versus zentrale Cyber-Sicherheit“ ... 28
1.5.6 Paradigmenwechsel „datengetriebene- versus ereignisgesteuerte-Sicherheit“ ... 28
1.5.7 Paradigmenwechsel „Zusammenarbeit versus Isolierung“ ... 28
1.6 Konzept der Wirksamkeit von Cyber-Sicherheitssystemen ... 29
1.6.1 Indirekte Angriffe auf die Werte ... 30
1.6.2 Stärke eines Cyber-Sicherheitsmechanismus gegen einen direkten Angriff ... 31
1.6.3 Überwindung des Cyber-Sicherheitsmechanismus durch einen direkten Angriff (unzureichende Wirkung) ... 32
1.6.4 Erfolgreiche Abwehr eines Cyber-Sicherheitsmechanismus durch einen direkten Angriff (ausreichende Wirkung) ... 32
1.7 Cyber-Sicherheitsbedürfnisse/Cyber-Sicherheitsziele ... 33
1.8 Cyber-Sicherheitsstrategien ... 34
1.8.1 Vermeiden von Angriffen ... 35
1.8.2 Entgegenwirken von Angriffen ... 38
1.8.3 Erkennen von Angriffen ... 39
1.8.4 Reaktion auf Angriffe ... 40
1.9 Angreifer und deren Motivationen ... 42
1.9.1 Angreifer Motivationen ... 43
1.9.2 Kategorien von Angreifern ... 43
1.10 Angriffsvektoren und Angriffsbeispiele ... 45
1.11 Das Pareto-Prinzip der Cyber-Sicherheit ... 49
1.12 Cyber-Sicherheitsschäden ... 50
1.13 Absichern des Cyber-Sicherheitsrisikos ... 52
1.14 Zusammenfassung ... 55
1.15 Übungsaufgaben ... 56
Literatur ... 59

2 Kryptografie ... 61
2.1 Grundlagen der Kryptografie ... 61
2.1.1 Grundlagen der Verschlüsselung ... 62
2.1.2 Definition eines kryptografischen Verfahrens ... 64
2.1.3 No Security by Obscurity ... 64
2.1.4 Die wichtigsten Begriffe in Kurzdefinition ... 65
2.1.5 Begriffe aus der Kryptoanalysis ... 65
2.1.6 Strategien der Analyse eines Kryptosystems ... 66

2.1.7 Bewertung der kryptografischen Stärke ... 67
2.1.8 Unterstützung bei der Einschätzung von Verfahren und Schlüssellängen ... 71
2.1.9 Zusammenfassung: Grundlagen der Kryptografie ... 71
2.2 Elementare Verschlüsselungsverfahren ... 72
2.2.1 Monoalphabetische Substitution ... 72
2.2.2 Homofone Substitution ... 73
2.2.3 Polyalphabetische Substitution ... 75
2.2.4 Transpositionsverfahren ... 76
2.2.5 Zusammenfassung: Elementare Verschlüsselungsverfahren ... 77
2.3 Der Einmal-Schlüssel ... 77
2.4 Symmetrische Verschlüsselungsverfahren ... 78
2.4.1 Data Encryption Standard (DES) ... 79
2.4.2 Advanced Encryption Standard (AES) ... 80
2.4.3 Zusammenfassung von symmetrischen Verschlüsselungsverfahren ... 83
2.5 Verwaltung von Schlüsseln (Key Management) ... 84
2.6 Blockverschlüsselung/Mode of Operation ... 86
2.6.1 Betriebsart: Electronic Code Book Mode (ECB-Mode) ... 87
2.6.2 Betriebsart: Cipher Block Chaining Mode (CBC-Mode) ... 87
2.6.3 Betriebsart: Cipher Feedback Mode (CFB-Mode) ... 89
2.6.4 Betriebsart: Output Feedback Mode (OFB-Mode) ... 90
2.6.5 Betriebsart: Counter Mode (CTR-Mode) ... 91
2.6.6 Betriebsart: Galois/Counter Mode (GCM-Mode) ... 92
2.6.7 Betriebsart: CCM-Mode (Counter with CBC-MAC) ... 93
2.6.8 Zusammenfassung: Modes of Operation ... 93
2.7 Steganografie ... 94
2.8 Asymmetrische Verschlüsselungsverfahren ... 95
2.8.1 Das RSA-Verfahren ... 98
2.8.2 Das Diffie-Hellman-Verfahren ... 100
2.8.3 Elliptische Kurven ... 102
2.8.4 Hybride Verschlüsselungsverfahren ... 102
2.9 Quantencomputer: Das Damoklesschwert der Verschlüsselung ... 103
2.10 One-Way-Hashfunktionen ... 104
2.10.1 Besondere Eigenschaften von Hashfunktionen ... 105
2.10.2 SHA-3 (SHA = Secure Hash Algorithm) ... 106
2.10.3 Message Authentication Code (MAC) ... 107
2.10.4 Keyed-Hashing for Message Authentication (HMAC) ... 107
2.11 Zusammenfassung ... 109
2.12 Übungsaufgaben ... 109
Literatur ... 117

3 Hardware-Sicherheitsmodule zum Schutz von Sicherheitsinformationen ... 119
3.1 Einleitung ... 119

3.2 Hardware-Sicherheitsmodul: Smartcards ... 120
3.3 Hardware-Sicherheitsmodul: Trusted Platform Module (TPM) ... 122
3.4 Hardware-Sicherheitsmodul: High-Level Security Module (HLSM) ... 124
3.5 Trusted Execution Environment (TEE) ... 127
3.6 Zusammenfassung: Kategorien von Hardware-Sicherheitsmodulen ... 127
3.7 Evaluierung und Zertifizierung für eine höhere Vertrauenswürdigkeit von Hardware-Sicherheitsmodulen ... 128
3.8 Key-Management von Hardware-Sicherheitsmodulen ... 129
3.8.1 Das Management von TPMs ... 129
3.8.2 Vier-Augen-Prinzip ... 129
3.9 Zusammenfassung ... 130
3.10 Übungsaufgaben ... 130
Literatur ... 132

4 Digitale Signatur, elektronische Zertifikate sowie Public Key-Infrastruktur (PKI) und PKI-enabled Application (PKA) ... 133
4.1 Digitale Signatur ... 133
4.1.1 Eigenhändige Unterschrift als Äquivalent zur digitalen Signatur ... 133
4.1.2 Digitale Signatur mithilfe eines Public Key-Verfahrens ... 135
4.2 Elektronische Zertifikate/digitale Zertifikate ... 137
4.3 Public Key-Infrastrukturen ... 140
4.3.1 Idee und Definition von Public Key-Infrastrukturen ... 141
4.3.2 Offene und geschlossene PKI-Systeme ... 145
4.3.3 Umsetzungskonzepte von Public Key-Infrastrukturen ... 148
4.4 Vertrauensmodelle von Public Key-Infrastrukturen ... 150
4.4.1 Vertrauensmodell: Übergeordnete CA (Wurzel-CA, Root CA) ... 150
4.4.2 Vertrauensmodell: n:n-Cross-Zertifizierung ... 151
4.4.3 Vertrauensmodell: 1:n Cross-Zertifizierung (Bridge CA) ... 152
4.4.4 Fazit ... 153
4.5 Gesetzlicher Hintergrund ... 153
4.6 PKI-enabled Application (Beispiele) ... 157
4.6.1 E-Mail-Sicherheit ... 157
4.6.2 Lotto – Online-Glückspiel ... 163
4.7 Zusammenfassung ... 165
4.8 Übungsaufgaben ... 166
Literatur ... 167

5 Identifikation und Authentifikation ... 169
5.1 Was ist eine Identifikation und Authentifikation? ... 169
5.1.1 Identifikation ... 169
5.1.2 Authentifikation ... 171
5.1.3 Klassen von Authentifizierungsverfahren ... 173

5.2 Identifikationsverfahren ... 174
5.2.1 Vorlage eines Personalausweises ... 175
5.2.2 Fernidentifizierung – Allgemeine Aspekte ... 175
5.2.3 Videoidentifikation ... 176
5.2.4 Das eID Verfahren des elektronischen Personalausweises ... 179
5.2.5 Das PostIdent-Verfahren der Deutschen Post AG ... 181
5.2.6 Vergleich der verschiedenen Identifikationsverfahren ... 182
5.2.7 Weitere Identifikationsverfahren ... 184
5.2.8 Abgeleitete Identitäten – vertrauenswürdige digitale Identität ... 186
5.3 Authentifikationsverfahren ... 187
5.3.1 Passwort-Verfahren ... 187
5.3.2 Einmal-Passwort-Verfahren ... 198
5.3.3 Challenge-Response-Verfahren ... 200
5.3.4 Biometrische Verfahren ... 202
5.3.5 Weitere unterstützende Faktoren (Reputation, Technologie, Standort, Zeit) ... 214
5.4 Multifaktor-Authentifizierung ... 216
5.5 Konzept der risikobasierten und adaptiven Authentifizierung ... 217
5.6 Modernes Multifaktor-Authentifizierungssystem und Identifikationsverfahren ... 218
5.7 Fast Identity Online Alliance (FIDO) ... 223
5.7.1 Ziele der FIDO Alliance ... 224
5.7.2 Die FIDO-Architektur ... 225
5.7.3 Authentifizierung des Nutzers ... 227
5.8 Identity Provider ... 227
5.8.1 OpenID ... 228
5.8.2 OAuth 2.0 ... 231
5.8.3 OpenID Connect ... 235
5.9 Anonymität im Cyber-Raum ... 236
5.10 Zusammenfassung ... 237
5.11 Übungsaufgaben ... 238
Literatur ... 239

6 Enterprise Identity und Access Management ... 241
6.1 Szenario eines Enterprise Identity and Access Management-Systems ... 243
6.2 Enterprise Identity and Access Management-Referenzmodell ... 244
6.3 Policies & Workflows ... 244
6.3.1 Policy Management ... 245
6.3.2 Workflow Management ... 246
6.3.3 Beispiel für Policies & Workflows ... 246
6.4 Repository Management ... 246
6.4.1 Auf einer Datenbank basierendes Directory ... 247
6.4.2 Metadirectory ... 247

6.4.3 Virtual Directory ... 248
6.4.4 Identity Repository ... 248
6.4.5 Policy Repository ... 248
6.4.6 Beispiel für Repository Management ... 248
6.5 Life Cycle Management ... 248
6.5.1 Identity-Administration ... 249
6.5.2 Provisionierung ... 249
6.5.3 Rollenmanagement ... 250
6.5.4 Privileged User Management ... 250
6.5.5 Delegierte Administration ... 251
6.5.6 Synchronisierung ... 251
6.5.7 Self-Service ... 251
6.5.8 Credential Management ... 252
6.5.9 Beispiel für Life Cycle Management ... 252
6.6 Access Management ... 252
6.6.1 Authentisierungs- und Authentifizierungs-Management ... 253
6.6.2 Autorisierungs-Management ... 253
6.6.3 Single Sign-On/Single Log-out ... 254
6.6.4 Access Control ... 255
6.6.5 Remote Access Control ... 255
6.6.6 Network Access Control ... 256
6.6.7 Policy Enforcement ... 256
6.6.8 Beispiel für Access Management ... 257
6.7 Information Protection ... 257
6.7.1 Secure Sharing ... 258
6.7.2 Information Rights Management ... 258
6.7.3 Content Security ... 258
6.7.4 Beispiel für Information Protection ... 259
6.8 Federation ... 259
6.8.1 Trust Management ... 259
6.8.2 Identity Federation ... 260
6.8.3 Beispiel für Federation ... 260
6.9 Compliance & Audit ... 260
6.9.1 Compliance Management ... 261
6.9.2 Monitoring ... 262
6.9.3 Reporting ... 262
6.9.4 Auditing ... 262
6.9.5 Beispiel für Compliance & Audit ... 262
6.10 Allgemeine Mehrwerte eines Enterprise Identity and Access Management-Systems ... 263
6.11 Zusammenfassung ... 266
6.12 Übungsaufgaben ... 266
Literatur ... 267

7 Trusted Computing ... 269
7.1 Einleitung ... 269
7.2 Trusted Computing auf den Punkt gebracht ... 272
7.2.1 Robustheit und Modularität ... 272
7.2.2 Integritätsüberprüfung ... 273
7.2.3 Trusted Process ... 274
7.2.4 Trusted Platform ... 275
7.3 Trusted Computing – Grundlagen ... 275
7.3.1 Kernelarchitekturen von Betriebssystemen ... 275
7.3.2 Core Root of Trust for Measurement (CRTM) ... 278
7.3.3 Identitäten von TPMs ... 279
7.3.4 TPM-Schlüssel und deren Eigenschaften ... 280
7.4 Trusted Computing-Funktionen ... 284
7.4.1 Authenticated Boot ... 285
7.4.2 Binding ... 286
7.4.3 Sealing (Erweiterung von Binding) ... 286
7.4.4 (Remote) Attestation (Beglaubigung, Überprüfung der Systemkonfiguration eines IT-Systems) ... 287
7.5 Trusted Platform (Security-Plattform, Sicherheitsplattform) ... 289
7.6 Beispielanwendungen ... 292
7.7 Trusted Network Connect (TNC) ... 296
7.7.1 Problemstellung ... 297
7.7.2 Anforderungen an heutige Netzwerke ... 298
7.7.3 Vertrauenswürdige Netzwerkverbindungen ... 298
7.7.4 Trusted Network Connect (TNC) im Detail ... 300
7.7.5 Anwendungsfelder ... 303
7.7.6 Kritische Diskussion ... 304
7.7.7 Zusammenfassung Trusted Network Connect (TNC) ... 306
7.8 Festlegung einer sicheren und vertrauenswürdigen Systemkonfiguration ... 306
7.9 Zusammenfassung ... 307
7.10 Übungsaufgaben ... 307
Literatur ... 308

8 Cyber-Sicherheit-Frühwarn- und Lagebildsysteme ... 309
8.1 Einleitung ... 309
8.2 Angriffe und ihre Durchführung ... 309
8.3 Idee eines Cyber-Sicherheit-Frühwarnsystems ... 317
8.3.1 Reaktionszeit für die Frühwarnung ... 317
8.3.2 Definition eines Cyber-Sicherheit-Frühwarnsystems ... 317
8.3.3 Obligatorische funktionelle Anforderungen ... 318
8.3.4 Asymmetrische Bedrohungen ... 318
8.4 Aufbau eines Cyber-Sicherheit-Frühwarnsystems ... 319
8.4.1 Rechtliche Rahmenbedingungen ... 319
8.4.2 Beteiligte Organisationen ... 319

8.5 Technische Realisierung eines Cyber-Sicherheit-Frühwarnsystems ... 320
8.5.1 Architektur ... 320
8.5.2 Sensoren ... 321
8.5.3 Analyse- und Erkennungsmodul ... 321
8.6 Prinzipielle Aspekte von Sensoren ... 323
8.6.1 Grundprinzip von Sensoren ... 324
8.6.2 Messmethoden ... 325
8.6.3 Ort der Messung ... 325
8.7 Diskussion unterschiedlicher Sensoren ... 326
8.7.1 NetFlow-Sensor/IPFIX-Sensor ... 327
8.7.2 Netzwerk-Sensor ... 329
8.7.3 SNMP-Sensor ... 332
8.7.4 Wireshark-Sensor ... 334
8.7.5 Honeypot-Sensor ... 336
8.7.6 Logdaten-Sensor ... 337
8.7.7 Verfügbarkeitssensor ... 339
8.8 Analysekonzepte ... 341
8.8.1 Erkennen von bekannten sicherheitsrelevanten Aktionen ... 341
8.8.2 Erkennen von Anomalien ... 341
8.9 Cyber-Sicherheit-Frühwarnprozess ... 343
8.10 Kommunikationslagebild ... 344
8.11 Zusammenfassung ... 351
8.12 Übungsaufgaben ... 351
Literatur ... 352

9 Firewall-Systeme ... 353
9.1 Bedrohungen im Netz ... 353
9.1.1 Angriffsmöglichkeiten in Kommunikationssystemen ... 354
9.1.2 Passive Angriffe ... 354
9.1.3 Aktive Angriffe ... 355
9.2 Idee und Definition von Firewall-Systemen ... 357
9.2.1 Elektronische Brandschutzmauer ... 358
9.2.2 Elektronischer Pförtner ... 358
9.3 Das Sicherheitskonzept ... 358
9.4 Aufgaben von Firewall-Systemen ... 359
9.5 Grundlage von Firewall-Systemen ... 360
9.6 Definition eines Firewall-Elements ... 367
9.7 Designkonzept aktiver Firewall-Elemente ... 371
9.8 Umsetzungsmöglichkeiten eines Firewall-Systems mit unterschiedlichen Firewall-Elementen ... 372
9.8.1 Packet Filter ... 372
9.8.2 Zustandsorientierte Packet Filter (stateful inspection) ... 375
9.8.3 Application Gateway/Proxy-Technik ... 377
9.9 Next-Generation-Firewall ... 381

9.10 Firewall-Konzepte ... 383
9.11 Konzeptionelle Möglichkeiten und Grenzen von Firewall-Systemen ... 386
9.11.1 Konzeptionelle Möglichkeiten eines Firewall-Systems ... 386
9.11.2 Konzeptionelle Grenzen eines Firewall-Systems ... 387
9.12 Das richtige Firewall-Konzept für jeden Anwendungsfall ... 390
9.13 Definition des Kommunikationsmodells mit integriertem Firewall-Element ... 392
9.14 Zusammenfassung ... 398
9.15 Übungsaufgaben ... 398
Literatur ... 401

10 IPSec-Verschlüsselung ... 403
10.1 Einleitung ... 403
10.2 IPSec Header ... 404
10.2.1 Authentication Header ... 405
10.2.2 Encapsulated Security Payload ... 406
10.3 Cyber-Sicherheitsdienste der IPSec-Header und Realisierungsformen ... 408
10.4 IPSec-Schlüsselmanagement ... 414
10.4.1 Manual Keying ... 414
10.4.2 Internet-Key-Exchange-Protocol (IKE) – Version 1 ... 414
10.5 Phasen und Modi von IKEv1 ... 416
10.5.1 Phase 1 (IKEv1): ISAKMP Security Association ... 416
10.5.2 Phase 2 (IKEv1): IPSec Security-Association ... 420
10.5.3 Phase 3: Integritätsgesicherte und verschlüsselte IP-Kommunikation ... 424
10.6 Phasen und Modi von IKEv2 ... 425
10.7 Anwendungsformen von IPSec-Lösungen ... 427
10.8 Protokollmitschnitt (IKEv1) ... 429
10.9 Zusammenfassung ... 436
10.10 Übungsaufgaben ... 436
Literatur ... 438

11 Transport Layer Security (TLS)/Secure Socket Layer (SSL) ... 439
11.1 Einleitung ... 439
11.2 Einbindung in die Kommunikationsarchitektur ... 440
11.3 Protokolle der TLS/SSL-Schicht ... 442
11.4 TLS/SSL-Zertifikate ... 455
11.5 Authentifikationsmethoden ... 457
11.6 Anwendungsformen von TLS/SSL-Lösungen ... 460
11.7 Protokollmitschnitt ... 462
11.8 TLS 1.3 ... 468
11.9 Zusammenfassung ... 471
11.10 Übungsaufgaben ... 472
Literatur ... 473

12 Cyber-Sicherheitsmaßnahmen gegen DDoS-Angriffe 475
12.1 Einleitung 475
12.2 Gezielte Überlastung von verfügbaren Ressourcen 477
12.3 Reflection und Amplification 478
12.4 Abwehrstrategien gegen Angriffe auf die Verfügbarkeit 479
12.4.1 Cyber-Sicherheitsrichtlinien zum Schutz vor Verfügbarkeitsangriffen 479
12.4.2 On-Site-Robustheitsmaßnahmen 480
12.4.3 Off-Site-Dienstleistungsmodelle 481
12.5 Präventiv gegen Beteiligung – Sichere Konfiguration von Diensten 486
12.6 Zusammenfassung 486
12.7 Übungsaufgaben 487
Literatur 487

13 E-Mail-Sicherheit 489
13.1 Einleitung 489
13.2 Generelle Cyber-Sicherheitsprobleme des E-Mail-Dienstes 490
13.3 E-Mail-Verschlüsselung 491
13.3.1 PGP und S/MIME sowie deren Unterschiede 492
13.3.2 Weitere Alternativen für E-Mail-Sicherheit 496
13.4 Spam-E-Mails 501
13.4.1 Definition und Hintergründe von Spam-Mails 501
13.4.2 Schäden, die durch Spam-Mails auftreten 502
13.4.3 Mechanismen zum Erkennen von Spam-Mails 503
13.4.4 Mechanismen zur Vermeidung von Spam-Mails 505
13.5 Zusammenfassung 507
13.6 Übungsaufgaben 507
Literatur 508

14 Blockchain-Technologie 509
14.1 Einleitung 509
14.2 Blockchain-Technologie auf den Punkt gebracht 509
14.3 Aufbau der Blockchain-Technologie 512
14.3.1 Element: Daten 512
14.3.2 Element: Block 513
14.3.3 Element: HashPrev 514
14.3.4 Element: Merkle Hash 515
14.3.5 Element: Transaktionen 516
14.3.6 Element: Node 519
14.3.7 Element: Blockchain-Teilnehmer 521
14.3.8 Element: Wallet 521
14.3.9 Element: Blockchain-Adresse 523
14.3.10 Prinzip: Keine „zentrale Instanz“ 524
14.3.11 Konsensfindungsverfahren 524
14.3.12 Struktur: Berechtigungsarchitektur 534

14.3.13 Ablauf der Verstetigung von Transaktionen 536
14.4 Hard und Soft Forks von Blockchains 536
14.5 Anwendungsformen und Anwendungen der Blockchain 541
14.6 Blockchain-as-a-Service 547
14.7 Sicherheit und Vertrauenswürdigkeit der Blockchain-Technologie 548
14.7.1 Sicherheit der Blockchain-Infrastruktur 549
14.7.2 Sicherheit der Blockchain-Anwendung 552
14.8 Gegenüberstellung PKI- und Blockchain-Technologien 555
14.9 Zusammenfassung 556
14.10 Übungsaufgaben 557
Literatur 558

15 Künstliche Intelligenz und Cyber-Sicherheit 561
15.1 Einleitung 561
15.2 Einordnung der Künstlichen Intelligenz 562
15.3 Erfolgsfaktoren der Künstlichen Intelligenz 563
15.4 Das Prinzip des Maschinellen Lernens 565
15.5 Qualität der Eingabedaten 566
15.6 Kategorien und Algorithmen des Maschinellen Lernens 569
15.6.1 Überwachtes Lernen 569
15.6.2 ML-Algorithmus: Support-Vector-Machine (SVM) 570
15.6.3 ML-Algorithmus: k-Nearest-Neighbor (kNN) 573
15.6.4 Unüberwachtes Lernen 576
15.6.5 ML-Algorithmus: k-Means-Algorithmus 577
15.6.6 ML-Algorithmus: Hierarchische Clustering-Verfahren 579
15.6.7 Künstliche Neuronale Netze (KNN) 580
15.6.8 Deep Learning 585
15.7 Anwendungsszenarien von KI und Cyber-Sicherheit 586
15.8 Manipulationen von Künstlicher Intelligenz 589
15.9 Beispiele von KI und Cyber-Sicherheit 594
15.9.1 Alert-System auf der Basis eines kontinuierlichen Lagebilds über die aktuelle Gefahrenlage im Online-Banking 594
15.9.2 Identifikation/Authentifikation eines Nutzers mittels Smartphone-Sensoren 600
15.9.3 Erkennung von netzwerkbasierten Angriffen mittels Künstlicher Intelligenz 602
15.10 Ethik und Künstliche Intelligenz 605
15.10.1 KI und Cyber-Sicherheit – eine Frage der Ethik? 606
15.10.2 Nachvollziehbarkeit von Entscheidungen als Prinzip 609
15.10.3 Ethik.KI.Tool 609
15.11 Zusammenfassung 611
15.12 Übungsaufgaben 612
Literatur 613

16 Social Web Cyber-Sicherheit ... 615
16.1 Einleitung ... 615
16.2 Soziale Netzwerke ... 616
16.3 Fake-News ... 618
16.3.1 Was sind Fake-News? ... 618
16.3.2 Social Bot (die digitale Propaganda-Maschine) ... 621
16.3.3 Wie können Fake-News erkannt werden? ... 622
16.4 Deep Fake ... 625
16.5 Filterblasen und Echokammern ... 626
16.6 Psychometrie bei sozialen Netzwerken ... 628
16.7 Cyber-Mobbing ... 629
16.8 Zusammenfassung ... 631
16.9 Übungsaufgaben ... 632
Literatur ... 632

17 Wirtschaftlichkeit von Cyber-Sicherheitsmaßnahmen ... 633
17.1 Einführung ... 633
17.2 Cyber-Sicherheit ... 635
17.2.1 Schutzbedarf von IT-Systemen ... 635
17.2.2 Wie sicher ist „sicher"? ... 635
17.2.3 Verwundbarkeit ... 636
17.3 Return on Security Investment RoSI – Nutzenaspekt ... 636
17.4 Beispielberechnung RoSI: Notebookverluste ... 638
17.5 Zusammenfassung ... 643
17.6 Übungsaufgaben ... 643
Literatur ... 644

18 Self-Sovereign Identity (SSI) ... 645
18.1 Self-Sovereign Identity (SSI) auf den Punkt gebracht ... 645
18.2 Die Architektur von Self-Sovereign Identity (SSI) ... 648
18.3 Decentralized Identifier (DID) ... 650
18.3.1 Das Konzept dezentralen Identitäten (DID) ... 650
18.3.2 Ziele und Prinzipien von DIDs ... 652
18.4 Verifiable Credential (VC) ... 652
18.5 Hyperledger Aries ... 654
18.6 Akteure: Self-Sovereign Identity (SSI) ... 656
18.6.1 Aussteller (Issuer) von digitalen Nachweisen ... 656
18.6.2 Nutzer (Holder) von verifizierbaren digitalen Nachweisen ... 657
18.6.3 Verifizierer, die digitale Nachweise für ihre Prozesse nutzen ... 658
18.7 SSI-Blockchain-Infrastruktur als Verifiable Data Registry (VDR) ... 659
18.8 Zero-Knowledge Proofs (ZKP) ... 661
18.8.1 Selective Disclosure ... 661
18.8.2 Predicate Proofs ... 662

18.8.3 Signature Blinding ... 663
18.8.4 Private Holder Binding ... 663
18.9 Anwendungsbeispiele von Self-Sovereign Identity ... 664
18.10 SSI-Ökosystem für digitale Identitäten in der Zukunft – Vorzüge und Vorbehalte ... 667
18.10.1 Digitalisierung und Akzeptanz der Bürger ... 667
18.10.2 Wirtschaftliche Relevanz eines SSI-Ökosystems für digitale Identitäten ... 668
18.10.3 Technologische Souveränität ... 669
18.11 Zusammenfassung ... 669
18.12 Übungsaufgaben ... 670
Literatur ... 671

19 Vertrauen und Vertrauenswürdigkeit ... 673
19.1 Zusammenhang zwischen Vertrauen, Vertrauenswürdigkeit und Cyber-Sicherheit ... 673
19.2 Vertrauen ... 674
19.3 Vertrauenswürdigkeitsmodell ... 675
19.3.1 Vertrauenswürdigkeit der IT-Lösung ... 678
19.3.2 Vertrauenswürdigkeit des Unternehmens ... 681
19.3.3 Vertrauenswürdigkeit von Domänen ... 685
19.3.4 Zusammenfassung: Vertrauenswürdigkeitsmodell ... 687
19.4 Mechanismen zur Vertrauensbildung ... 687
19.4.1 Eigene emotionale Referenz ... 687
19.4.2 Neutrale Referenz ... 688
19.4.3 Zusammenfassung: Mechanismen zur Vertrauensbildung ... 690
19.5 Vertrauenswürdigkeitstechnologie ... 691
19.6 Zusammenfassung ... 693
19.7 Übungsaufgaben ... 693
Literatur ... 693

20 Weitere Aspekte der Cyber-Sicherheit ... 695
20.1 DNS over HTTPS (DoH) ... 695
20.2 Backup ... 697
20.3 Chancen und Risiken von Smart Home ... 700
20.4 Risiken und Sicherheit eines Homeoffice ... 705
20.4.1 Risiken beim Homeoffice ... 705
20.4.2 Sicherheitsmaßnahmen für das Homeoffice ... 708
20.5 Upload-Filter ... 712
20.6 Übungsaufgaben ... 715
Literatur ... 716

21 Glossar ... 717

Symbole ... 737

Stichwortverzeichnis ... 741