Inhaltsverzeichnis

1 Sichtweisen auf die Cyber-Sicherheit 1
1.1 Einleitung 1
1.2 Cyber-Sicherheitsprobleme 2
1.2.1 Cyber-Sicherheitsproblem: „Zu viele Schwachstellen in Software“ 3
1.2.2 Cyber-Sicherheitsproblem: „Ungenügender Schutz vor Malware“ 4
1.2.3 Cyber-Sicherheitsproblem: „Keine internationalen Lösungen für Identifikation und Authentifikation“ 6
1.2.4 Cyber-Sicherheitsproblem: „Unsichere Webseiten im Internet“ 7
1.2.5 Cyber-Sicherheitsproblem: „Gefahren durch die Nutzung mobiler Geräte“ 7
1.2.6 Cyber-Sicherheitsproblem: „Eine E-Mail ist wie eine Postkarte!“ 9
1.2.7 Cyber-Sicherheitsproblem: „Geschäftsmodell: Bezahlen mit persönlichen Daten“ 9
1.2.8 Cyber-Sicherheitsproblem: „Internetnutzer haben zu wenig Internet-Kompetenz“ 10
1.2.9 Cyber-Sicherheitsproblem: „Manipulierte IT und IT-Sicherheitstechnologien“ 11
1.2.10 Cyber-Sicherheitsproblem: „Unsichere IoT-Geräte“ 11
1.2.11 Cyber-Sicherheitsproblem: „Fake News“ und weitere unerwünschte Inhalte 13
1.3 Problematische Rahmenbedingungen 14

Bibliografische Informationen
http://d-nb.info/1183834152

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

1.4 Gesellschaftliche Sichtweise auf die Cyber-Sicherheitsprobleme ... 14
1.4.1 Privatsphäre und Datenschutz ... 14
1.4.2 Selbstbestimmung und Autonomie ... 16
1.4.3 Wirtschaftsspionage ... 17
1.4.4 Cyberwar ... 17
1.5 Herausforderungen der Cyber-Sicherheit ... 18
1.5.1 Paradigmenwechsel „Verantwortung versus Gleichgültigkeit" ... 18
1.5.2 Paradigmenwechsel „Proaktive versus reaktive Cyber-Sicherheitslösungen" ... 19
1.5.3 Paradigmenwechsel „Objekt-Sicherheit versus Perimeter-Sicherheit" ... 20
1.5.4 Paradigmenwechsel „Cloud-Service versus Lokal-IT" ... 21
1.5.5 Paradigmenwechsel „Dezentrale versus zentrale Cyber-Sicherheit" ... 21
1.5.6 Paradigmenwechsel „datengetriebene- versus eventgetriebene-Sicherheit" ... 21
1.5.7 Paradigmenwechsel „Zusammenarbeit versus Isolierung" ... 22
1.6 Konzept der Wirksamkeit von Cyber-Sicherheitssystemen ... 22
1.7 Cyber-Sicherheitsstrategien ... 26
1.7.1 Vermeiden von Angriffen ... 26
1.7.2 Entgegenwirken von Angriffen ... 28
1.7.3 Erkennen von Angriffen ... 29
1.8 Angreifer und deren Motivationen ... 30
1.9 Cyber-Sicherheitsbedürfnisse ... 32
1.10 Das Pareto-Prinzip der Cyber-Sicherheit ... 33
1.11 Cyber-Sicherheitsrisiko ... 34
1.12 Zusammenfassung ... 37
1.13 Übungsaufgaben ... 37
Literatur ... 41

2 Kryptografie ... 43
2.1 Grundlagen der Kryptografie ... 43
2.1.1 Grundlagen der Verschlüsselung ... 44
2.1.2 Definition eines kryptografischen Verfahrens ... 46
2.1.3 No Security by Obscurity ... 46
2.1.4 Die wichtigsten Begriffe in Kurzdefinition ... 47
2.1.5 Begriffe aus der Kryptoanalysis ... 48

2.1.6 Strategien der Analyse eines Kryptosystems ... 48
2.1.7 Bewertung der kryptografischen Stärke ... 50
2.1.8 Unterstützung bei der Einschätzung von Verfahren und Schlüssellängen ... 53
2.1.9 Zusammenfassung: Grundlagen der Kryptografie ... 53
2.1.10 Monoalphabetische Substitution ... 54
2.1.11 Homofone Substitution ... 55
2.1.12 Polyalphabetische Substitution ... 57
2.1.13 Transpositionsverfahren ... 58
2.1.14 Zusammenfassung: Elementare Verschlüsselungsverfahren ... 59
2.1.15 Data Encryption Standard ... 61
2.1.16 Advanced Encryption Standard ... 62
2.1.17 Verwaltung von Schlüsseln (Key Management) ... 66
2.1.18 Betriebsart: Electronic Code Book Mode (ECB-Mode) ... 68
2.1.19 Betriebsart: Cipher Block Chaining Mode (CBC-Mode) ... 69
2.1.20 Betriebsart: Cipher Feedback Mode (CFB-Mode) ... 70
2.1.21 Betriebsart: Output Feedback Mode (OFB-Mode) ... 71
2.1.22 Betriebsart: Counter Mode (CTR-Mode) ... 72
2.1.23 Betriebsart: Galois/Counter Mode (GCM-Mode) ... 73
2.1.24 Modes of Operation: Zusammenfassung ... 74
2.2 Asymmetrische Verschlüsselungsverfahren ... 77
2.2.1 Das RSA-Verfahren ... 79
2.2.2 Das Diffie-Hellman-Verfahren ... 82
2.2.3 Elliptische Kurven ... 83
2.2.4 Hybride Verschlüsselungsverfahren ... 84
2.3 Quantencomputer: Das Damoklesschwert der Verschlüsselung ... 84
2.4 One-Way-Hashfunktionen ... 86
2.4.1 Besondere Eigenschaften von Hashfunktionen ... 87
2.4.2 SHA-3 (SHA = Secure Hash Algorithm) ... 88
2.4.3 Message Authentication Code (MAC) ... 88
2.4.4 Keyed-Hashing for Message Authentication (HMAC) ... 89
Literatur ... 99

3 Hardware-Sicherheitsmodule zum Schutz von sicherheitsrelevanten Informationen ... 101
3.1 Einleitung ... 101
3.2 Hardware-Sicherheitsmodul: Smartcards ... 102
3.3 Hardware-Sicherheitsmodul: Trusted Platform Module (TPM) ... 104
3.4 Hardware-Sicherheitsmodul: High-Level Security Module (HLSM) ... 106
3.5 Zusammenfassung: Kategorien von Hardware-Sicherheitsmodulen ... 109
3.6 Evaluierung und Zertifizierung für eine höhere Vertrauenswürdigkeit von Hardware-Sicherheitsmodulen ... 110
3.7 Key-Management von Hardware-Sicherheitsmodulen ... 110
3.7.1 Das Management von TPMs ... 111
3.7.2 Vier-Augen-Prinzip ... 111
3.8 Zusammenfassung ... 111
3.9 Übungsaufgaben ... 112
Literatur ... 114

4 Digitale Signatur, elektronische Zertifikate sowie Public Key-Infrastruktur (PKI) und PKI-enabled Application (PKA) ... 115
4.1 Digitale Signatur ... 115
4.2 Elektronische Zertifikate/digitale Zertifikate ... 119
4.3 Public Key-Infrastrukturen ... 122
4.3.1 Idee und Definition von Public Key-Infrastrukturen ... 123
4.3.2 Offene und geschlossene PKI-Systeme ... 127
4.3.3 Umsetzungskonzepte von Public Key-Infrastrukturen ... 130
4.4 Vertrauensmodelle von Public Key-Infrastrukturen ... 131
4.4.1 Vertrauensmodell: Übergeordnete CA (Wurzel-CA, Root CA) ... 132
4.4.2 Vertrauensmodell B: n:n-Cross-Zertifizierung ... 133
4.4.3 Vertrauensmodell: 1:n Cross-Zertifizierung (Bridge CA) ... 133
4.5 Gesetzlicher Hintergrund ... 134
4.6 PKI-enabled Application ... 138
4.6.1 E-Mail-Sicherheit ... 138
4.6.2 Lotto – Online-Glückspiel ... 145
4.7 Zusammenfassung ... 147
4.8 Übungsaufgaben ... 147
Literatur ... 148

5 Identifikation und Authentifikation 151
5.1 Was ist eine Identifikation und Authentifikation? 151
5.1.1 Identifikation 151
5.1.2 Authentifikation 152
5.1.3 Klassen von Authentifizierungsverfahren 153
5.2 Identifikationsverfahren 155
5.2.1 Vorlage eines Personalausweises 155
5.2.2 Fernidentifizierung – Allgemeine Aspekte 155
5.2.3 Videoidentifikation 156
5.2.4 Das eID Verfahren des elektronischen Personalausweises 159
5.2.5 Das PostIdent-Verfahren der Deutschen Post AG 161
5.2.6 Vergleich der verschiedenen Identifikationsverfahren 162
5.2.7 Weitere Identifikationsverfahren 164
5.2.8 Abgeleitete Identitäten 165
5.3 Authentifikationsverfahren 166
5.3.1 Passwort-Verfahren 167
5.3.2 Einmal-Passwort-Verfahren 178
5.3.3 Challenge-Response-Verfahren 179
5.3.4 Biometrische Verfahren 181
5.4 Mehrfaktor-Authentifizierung 187
5.5 Konzept der risikobasierten und adaptiven Authentifizierung 189
5.6 Modernes Multifaktor-Authentifizierungssystem und Identifikationsverfahren 190
5.7 Fast Identity Online Alliance (FIDO) 197
5.7.1 Ziele der FIDO Alliance 197
5.7.2 Die FIDO-Architektur 198
5.7.3 Authentifizierung des Nutzers 200
5.8 Identity Provider 201
5.8.1 OpenID 201
5.8.2 OAuth 2.0 204
5.8.3 OpenID Connect 208
5.9 Zusammenfassung 209
5.10 Übungsaufgaben 209
Literatur 210

6 Enterprise Identity und Access Management 213
6.1 Szenario eines Enterprise Identity and Access Management-Systems 215
6.2 Enterprise Identity and Access Management-Referenzmodell 215

6.3 Policys & Workflows ... 218
6.3.1 Policy Management ... 219
6.3.2 Workflow Management ... 219
6.3.3 Beispiel für Policys & Workflows ... 219
6.4 Repository Management ... 219
6.4.1 Auf einer Datenbank basierendes Directory ... 220
6.4.2 Metadirectory ... 220
6.4.3 Virtual Directory ... 221
6.4.4 Identity Repository ... 221
6.4.5 Policy Repository ... 221
6.4.6 Beispiel für Repository Management ... 221
6.5 Life Cycle Management ... 222
6.5.1 Identity-Administration ... 222
6.5.2 Provisionierung ... 223
6.5.3 Rollenmanagement ... 223
6.5.4 Privileged User Management ... 224
6.5.5 Delegierte Administration ... 224
6.5.6 Synchronisierung ... 224
6.5.7 Self-Service ... 225
6.5.8 Credential Management ... 225
6.5.9 Beispiel für Life Cycle Management ... 225
6.6 Access Management ... 226
6.6.1 Authentisierungs- und Authentifizierungs-Management ... 226
6.6.2 Autorisierungs-Management ... 227
6.6.3 Single Sign-On/Single Log-out ... 228
6.6.4 Access Control ... 228
6.6.5 Remote Access Control ... 229
6.6.6 Network Access Control ... 229
6.6.7 Policy Enforcement ... 230
6.6.8 Beispiel für Access Management ... 230
6.7 Information Protection ... 230
6.7.1 Secure Sharing ... 231
6.7.2 Information Rights Management ... 232
6.7.3 Content Security ... 232
6.7.4 Beispiel für Information Protection ... 232
6.8 Federation ... 232
6.8.1 Trust Management ... 233
6.8.2 Identity Federation ... 233
6.8.3 Beispiel für Federation ... 234
6.9 Compliance & Audit ... 234
6.9.1 Compliance Management ... 235
6.9.2 Monitoring ... 235
6.9.3 Reporting ... 235
6.9.4 Auditing ... 236
6.9.5 Beispiel für Compliance & Audit ... 236

6.10 Allgemeine Mehrwerte eines Enterprise Identity and Access Management-Systems ... 236
6.11 Zusammenfassung ... 239
6.12 Übungsaufgaben ... 239
Literatur ... 240

7 Trusted Computing ... 241
7.1 Einleitung ... 241
7.2 Trusted Computing auf den Punkt gebracht ... 244
7.2.1 Robustheit und Modularität ... 244
7.2.2 Integritätsüberprüfung ... 245
7.2.3 Trusted Process ... 246
7.2.4 Trusted Plattform ... 247
7.3 Trusted Computing – Grundlagen ... 247
7.3.1 Kernelarchitekturen von Betriebssystemen ... 247
7.3.2 Core Root of Trust for Measurement (CRTM) ... 250
7.3.3 Identitäten von TPMs ... 251
7.3.4 TPM-Schlüssel und deren Eigenschaften ... 252
7.3.5 Trusted Computing-Funktionen ... 256
7.3.6 Trusted Platform (Security-Plattform, Sicherheitsplattform) ... 260
7.3.7 Beispielanwendungen ... 263
7.4 Trusted Network Connect (TNC) ... 268
7.4.1 Problemstellung ... 268
7.4.2 Anforderungen an heutige Netzwerke ... 270
7.4.3 Vertrauenswürdige Netzwerkverbindungen ... 270
7.4.4 Trusted Network Connect (TNC) im Detail ... 272
7.4.5 Anwendungsfelder ... 275
7.4.6 Kritische Diskussion ... 276
7.4.7 Fazit: Trusted Network Connect (TNC) ... 278
7.5 Festlegung einer sicheren und vertrauenswürdigen Systemkonfiguration ... 278
7.6 Zusammenfassung ... 279
7.7 Übungsaufgaben ... 279
Literatur ... 280

8 Cyber-Sicherheit-Frühwarn- und Lagebildsysteme ... 281
8.1 Einleitung ... 281
8.2 Angriffe und ihre Durchführung ... 281
8.3 Idee eines Cyber-Sicherheit Frühwarnsystems ... 287
8.3.1 Reaktionszeit für die Frühwarnung ... 287
8.3.2 Definition eines Cyber-Sicherheit Frühwarnsystems ... 288
8.3.3 Obligatorische funktionelle Anforderungen ... 288
8.3.4 Asymmetrische Bedrohungen ... 289

8.4 Aufbau eines Cyber-Sicherheit Frühwarnsystems 289
8.4.1 Rechtliche Rahmenbedingungen 290
8.4.2 Beteiligte Organisationen 290
8.5 Technische Realisierung eines Cyber-Sicherheit Frühwarnsystems 290
8.5.1 Architektur 290
8.5.2 Sensoren 291
8.5.3 Analyse- und Erkennungsmodul 292
8.6 Prinzipielle Aspekte von Sensoren 294
8.6.1 Grundprinzip von Sensoren 294
8.6.2 Messmethoden 296
8.6.3 Ort der Messung 296
8.7 Diskussion unterschiedlicher Sensoren 297
8.7.1 NetFlow-Sensor 297
8.7.2 Netzwerk-Sensor 299
8.7.3 SNMP-Sensor 303
8.7.4 Wireshark-Sensor 305
8.7.5 Honeypot-Sensor 306
8.7.6 Logdaten-Sensor 308
8.7.7 Verfügbarkeitssensor 310
8.8 Analysekonzepte 311
8.8.1 Erkennen von bekannten sicherheitsrelevanten Aktionen 311
8.8.2 Erkennen von Anomalien 312
8.9 Cyber-Sicherheit-Frühwarnprozess 313
8.10 Kommunikationslagebild 314
8.11 Zusammenfassung 321
8.12 Übungsaufgaben 321
Literatur 323

9 Firewall-Systeme 325
9.1 Bedrohungen im Netz 325
9.1.1 Angriffsmöglichkeiten in Kommunikationssystemen 325
9.1.2 Passive Angriffe 326
9.1.3 Aktive Angriffe 327
9.2 Idee und Definition von Firewall-Systemen 329
9.2.1 Elektronische Brandschutzmauer 330
9.2.2 Elektronischer Pförtner 330
9.3 Das Sicherheitskonzept 330
9.4 Aufgaben von Firewall-Systemen 331
9.5 Grundlage von Firewall-Systemen 333
9.6 Definition eines Firewall-Elements 340
9.7 Designkonzept aktiver Firewall-Elemente 343
9.8 Packet Filter 345

9.9 Zustandsorientierte Packet Filter (stateful inspection) 347
9.10 Application Gateway/Proxy-Technik 349
9.11 Next-Generation-Firewall 353
9.12 Firewall-Konzepte 355
9.13 Konzeptionelle Möglichkeiten und Grenzen von Firewall-Systemen 357
9.13.1 Common Point of Trust 357
9.13.2 Konzeptionelle Grenzen eines Firewall-Systems 359
9.14 Das richtige Firewall-Konzept für jeden Anwendungsfall 361
9.15 Definition des Kommunikationsmodells mit integriertem Firewall-Element 364
9.16 Zusammenfassung 369
9.17 Übungsaufgaben 370
Literatur 372

10 IPSec-Verschlüsselung 373
10.1 Einleitung 373
10.2 IPSec Header 374
10.2.1 Authentication Header 375
10.2.2 Encapsulated Security Payload 376
10.3 Cyber-Sicherheitsdienste der IPSec-Header und Realisierungsformen 378
10.4 IPSec-Schlüsselmanagement 383
10.4.1 Manual Keying 384
10.4.2 Internet-Key-Exchange-Protocol (IKE) 384
10.5 Anwendungsformen von IPSec-Lösungen 395
10.6 Protokollmitschnitt 397
10.7 Zusammenfassung 403
10.8 Übungsaufgaben 403
Literatur 405

11 Transport Layer Security (TLS)/Secure Socket Layer (SSL) 407
11.1 Einleitung 407
11.2 Einbindung in die Kommunikationsarchitektur 408
11.3 Protokolle der TLS/SSL-Schicht 410
11.4 TLS/SSL-Zertifikate 424
11.5 Authentifikationsmethoden 426
11.6 Anwendungsformen von TLS/SSL-Lösungen 428
11.7 Protokollmitschnitt 430
11.8 Zusammenfassung 437
11.9 Übungsaufgaben 437
Literatur 438

12 Cyber-Sicherheitsmaßnahmen gegen DDoS-Angriffe 439
12.1 Einleitung 439
12.2 Gezielte Überlastung 441
12.3 Reflection und Amplification 442
12.4 Abwehrstrategien gegen Angriffe auf die Verfügbarkeit 443
12.4.1 Cyber-Sicherheitsrichtlinien zum Schutz vor Verfügbarkeitsangriffen 443
12.4.2 On-Site-Robustheitsmaßnahmen 444
12.4.3 Off-Site-Dienstleistungsmodelle 446
12.5 Präventiv gegen Beteiligung – Sichere Konfiguration von Diensten 450
12.6 Zusammenfassung 450
12.7 Übungsaufgaben 451
Literatur 451

13 E-Mail-Sicherheit 453
13.1 Einleitung 453
13.2 Generelle Cyber-Sicherheitsprobleme des E-Mail-Dienstes 454
13.3 E-Mail-Verschlüsselung 455
13.3.1 PGP und S/MIME sowie deren Unterschiede 456
13.3.2 Weitere Alternativen für E-Mail-Sicherheit 460
13.4 Zusammenfassung 466
13.5 Übungsaufgaben 466
Literatur 466

14 Blockchain-Technologie 467
14.1 Einleitung 467
14.2 Aufbau der Blockchain-Technologie 470
14.2.1 Element: Daten 470
14.2.2 Element: Block 471
14.2.3 Element: HashPrev 472
14.2.4 Element: Merkle Hash 473
14.2.5 Element: Transaktionen 474
14.2.6 Element: Node 477
14.2.7 Element: Wallet 478
14.2.8 Element: Blockchain-Adresse 480
14.2.9 Prinzip: Keine „zentrale Instanz" 481
14.2.10 Konsensfindungsverfahren 482
14.2.11 Struktur: Berechtigungsarchitektur 490
14.3 Hard und Soft Forks von Blockchains 492
14.4 Anwendungsformen und Anwendungen der Blockchain 501

14.5 Blockchain-as-a-Service 507
14.6 Sicherheit und Vertrauenswürdigkeit der Blockchain-Technologie 507
14.6.1 Sicherheit der Blockchain-Infrastruktur 508
14.6.2 Sicherheit der Blockchain-Anwendung 512
14.7 Gegenüberstellung PKI- und Blockchain-Technologien 514
14.8 Zusammenfassung 516
14.9 Übungsaufgaben 517
Literatur 519

15 Künstliche Intelligenz und Cyber-Sicherheit 521
15.1 Einleitung 521
15.2 Einordnung der Künstlichen Intelligenz 522
15.3 Erfolgsfaktoren der Künstlichen Intelligenz 523
15.4 Das Prinzip des Maschinellen Lernens 525
15.5 Kategorien und Algorithmen des Maschinellen Lernens 526
15.5.1 ML-Algorithmus: Support-Vector-Machine (SVM) 526
15.5.2 ML-Algorithmus: k-Nearest-Neighbor (kNN) 530
15.5.3 ML-Algorithmus: k-Means-Algorithmus 533
15.5.4 ML-Algorithmus: Hierarchische Clustering-Verfahren 535
15.5.5 Künstliche Neuronale Netze (KNN) 536
15.5.6 Deep Learning 541
15.6 Anwendungsszenarien von KI und Cyber-Sicherheit 542
15.7 Manipulationen von Künstlicher Intelligenz 545
15.8 Beispiele von KI und Cyber-Sicherheit 546
15.8.1 Alert-System auf der Basis eines kontinuierlichen Lagebilds über die aktuelle Gefahrenlage im Online-Banking 546
15.8.2 Identifikation/Authentifikation eines Nutzers mittels Smartphone- Sensoren 552
15.8.3 Erkennung von netzwerkbasierten Angriffen mittels Künstlicher Intelligenz 554
15.9 Zusammenfassung 557
15.10 Übungsaufgaben 558
Literatur 558

16 Social Web Cyber-Sicherheit 561
16.1 Soziale Netzwerke 562
16.2 Fake-News 564
16.2.1 Was sind Fake-News? 564
16.2.2 Social Bot (die digitale Propaganda-Maschine) 565

16.3 Filterblasen und Echokammern ... 569
16.4 Psychometrie bei sozialen Netzwerken ... 570
16.5 Zusammenfassung ... 571
16.6 Übungsaufgaben ... 571
Literatur ... 572

17 Wirtschaftlichkeit von Cyber-Sicherheitsmaßnahmen ... 573
17.1 Einführung ... 573
17.2 Cyber-Sicherheit ... 574
17.2.1 Schutzbedarf von IT-Systemen ... 574
17.2.2 Wie sicher ist „sicher"? ... 575
17.2.3 Verwundbarkeit ... 576
17.3 Return on Security Investment RoSI – Nutzenaspekt ... 576
17.4 Beispielberechnung RoSI: Notebookverluste ... 578
17.5 Zusammenfassung ... 582
17.6 Übungsaufgaben ... 582
Literatur ... 583

Anhang ... 585

Stichwortverzeichnis ... 589