1 Einführung 1
1.1 Warum IT-Sicherheit . . . 1
1.2 Ziele von IT-Sicherheit . . . 2
1.3 Angriffe auf IT-Sicherheit . . . 5
1.3.1 Angriffsarten . . . 5
1.3.2 Schwachstellen . . . 6
1.3.3 Ziele eines Angriffs . . . 7
1.4 Risiken und Unsicherheit . . . 7
1.5 IT-Sicherheit in der Praxis . . . 9
1.6 Organisatorische Grundlagen der IT-Sicherheit . . . 10
1.6.1 Rahmenbedingungen . . . 10
1.6.2 IT-Sicherheit als Prozess . . . 10
1.7 Rechtliche Grundlagen und Rahmenbedingungen in Deutschland . . . 11
1.7.1 Bundesdatenschutzgesetz . . . 11
1.7.2 Telekommunikationsgesetz . . . 12
1.7.3 Telemediengesetz . . . 13
1.7.4 Handelsgesetzbuch . . . 13
1.7.5 Bundesamt für Sicherheit in der Informationstechnik . . . 13
1.8 Zusammenfassung . . . 15
1.9 Übungsaufgaben . . . 15
1.9.1 Wiederholungsaufgaben . . . 15
1.9.2 Weiterführende Aufgaben . . . 16

2 Kryptographische Prinzipien und Methoden 17
2.1 Grundlagen . . . 17
2.1.1 Definition . . . 17
2.1.2 Modell . . . 18
2.2 Verschlüsselungsverfahren . . . 20
2.2.1 Vom Klartext zum Chiffretext . . . 20
2.2.2 Sicherheit von Verschlüsselungsverfahren . . . 21
2.2.2.1 Kryptanalysis . . . 21
2.2.2.2 Ein absolut sicheres Verfahren . . . 23
2.3 Symmetrische Verfahren und Public-Key-Verfahren . . . 25
2.3.1 Grundlagen . . . 25
2.3.2 Symmetrische Verfahren . . . 25
2.3.3 Public-Key-Verfahren . . . 27
2.3.4 Hybride Verfahren . . . 29

2.4 Betriebsarten . . . 31
2.4.1 Electronic Code Book . . . 31
2.4.2 Cipher Block Chaining . . . 32
2.4.3 Cipher Feedback Mode und Output Feedback Mode . . . 33
2.4.4 Counter Mode . . . 35
2.5 Zusammenfassung . . . 36
2.6 Übungsaufgaben . . . 37
2.6.1 Wiederholungsaufgaben . . . 37
2.6.2 Weiterführende Aufgaben . . . 37

3 Authentifikation **39**
3.1 Grundlagen . . . 39
3.2 Mögliche Faktoren zur Authentifikation . . . 40
3.3 Passwörter . . . 41
3.3.1 Größe des Passwortraums . . . 41
3.3.2 Sicherheit der Passwortspeicherung beim Anwender und im System . . . 43
3.3.3 Sicherheit der Passworteingabe und Übertragung . . . 45
3.3.4 Passwörter – Eine Sicherheitslücke? . . . 46
3.4 Tokens und Smart-Cards . . . 47
3.5 Biometrie . . . 48
3.6 Kryptographische Methoden . . . 50
3.6.1 Authentifikation von Benutzern und Maschinen . . . 50
3.6.2 Digitale Signatur . . . 52
3.6.3 Infrastrukturen zur Authentifikation . . . 54
3.6.3.1 Zertifikate und Certificate Authorities . . . 54
3.6.3.2 Zertifikate in der Praxis: X.509 . . . 57
3.6.3.3 Beispiel: X.509 Zertifikate mit OpenSSL selbst erstellen . . . 59
3.6.3.4 Web of Trust . . . 65
3.7 Zusammenfassung . . . 65
3.8 Übungsaufgaben . . . 66
3.8.1 Wiederholungsaufgaben . . . 66
3.8.2 Weiterführende Aufgaben . . . 67

4 Betriebssysteme und ihre Sicherheitsaufgaben **69**
4.1 Aufgaben und Aufbau von Betriebssystemen . . . 69
4.2 Systemadministratoren . . . 71
4.3 Rechtevergabe und Zugriffskontrolle am Beispiel Dateisystem . . . 72
4.4 Trusted Computing . . . 77
4.5 Monitoring und Logging . . . 78
4.6 Absichern des Systems gegen Angriffe . . . 78
4.7 Zusammenfassung . . . 79
4.8 Übungsaufgaben . . . 80
4.8.1 Wiederholungsaufgaben . . . 80
4.8.2 Weiterführende Aufgaben . . . 80

5 Anwendungen **83**
5.1 Einführung . . . 83
5.2 Buffer Overflows . . . 84
5.2.1 Das Problem . . . 84
5.2.2 Schutzmaßnahmen . . . 86
5.3 Race Conditions . . . 86
5.4 Software aus dem Internet . . . 88
5.4.1 Downloads . . . 88
5.4.2 Aktive Inhalte . . . 88
5.4.2.1 Einführung . . . 88
5.4.2.2 Java und Java-Applets . . . 89
5.4.2.3 JavaScript . . . 91
5.4.2.4 ActiveX Control . . . 91
5.5 Zusammenfassung . . . 91
5.6 Übungsaufgaben . . . 92
5.6.1 Wiederholungsaufgaben . . . 92
5.6.2 Weiterführende Aufgaben . . . 92

6 Malware **93**
6.1 Einführung . . . 93
6.2 Schaden . . . 94
6.3 Verbreitung und Funktionsweise . . . 95
6.3.1 Verbreitung . . . 95
6.3.2 Funktionsweise . . . 96
6.3.2.1 Viren . . . 96
6.3.2.2 Würmer . . . 97
6.3.2.3 Backdoors und Root Kits . . . 98
6.3.2.4 Zombies . . . 98
6.4 Schutzmaßnahmen und Entfernung von Malware . . . 99
6.4.1 Schutzmaßnahmen . . . 99
6.4.1.1 Virenscanner . . . 99
6.4.1.2 Systemkonfiguration, Dienste und Einstellungen . . . 99
6.4.1.3 Patches und Updates . . . 100
6.4.1.4 Heterogenität . . . 100
6.4.1.5 Firewalls und Filtermechanismen . . . 100
6.4.1.6 Vorsichtige Benutzer . . . 101
6.4.2 Entfernung . . . 101
6.5 Zusammenfassung . . . 102
6.6 Übungsaufgaben . . . 102
6.6.1 Wiederholungsaufgaben . . . 102
6.6.2 Weiterführende Aufgaben . . . 103

7 Netzwerke und Netzwerkprotokolle **105**
7.1 Grundlagen . . . 105

10.4 IPsec . . . 198
10.4.1 Einführung . . . 198
10.4.2 Das AH-Protokoll . . . 200
10.4.3 Das ESP-Protokoll . . . 202
10.4.4 Aufbau und Verwaltung von SAs und Schlüsselmanagement . . . 205
10.4.5 Praktisches Beispiel . . . 208
10.5 VPN-Technologien und Klassifikation . . . 211
10.6 Risiken bei der Verwendung von VPNs . . . 213
10.6.1 Split Tunneling . . . 213
10.6.2 Öffentliche Zugangsnetze für Endsysteme . . . 214
10.7 Zusammenfassung . . . 216
10.8 Übungsaufgaben . . . 217
10.8.1 Wiederholungsaufgaben . . . 217
10.8.2 Weiterführende Aufgaben . . . 217

11 Netzwerküberwachung **219**
11.1 Grundlagen . . . 219
11.2 Intrusion Detection . . . 220
11.2.1 Einführung . . . 220
11.2.2 Architektur und Komponenten eines netzwerkbasierten IDS . . . 222
11.2.3 Netzwerkbasierte IDS und Paketfilter . . . 224
11.2.4 Beispiel für die Verwendung eines IDS . . . 225
11.3 Scannen . . . 227
11.3.1 Einführung . . . 227
11.3.2 Finden von Geräten im Netz . . . 228
11.3.2.1 Ping-Sweep . . . 228
11.3.2.2 Address Resolution Protocol . . . 229
11.3.2.3 Domain Name Service . . . 230
11.3.3 Portscanning . . . 230
11.3.3.1 Prinzipielle Vorgehensweise . . . 230
11.3.3.2 TCP-Connect-Scan . . . 230
11.3.3.3 TCP-SYN-Scan . . . 232
11.3.3.4 Weitere TCP-Scans . . . 232
11.3.3.5 OS-Fingerprinting . . . 233
11.3.4 Schutz vor Scanning . . . 233
11.3.5 Scanning zum Schutz des Netzes . . . 234
11.4 Zusammenfassung . . . 235
11.5 Übungsaufgaben . . . 236
11.5.1 Wiederholungsaufgaben . . . 236
11.5.2 Weiterführende Aufgaben . . . 236

12 Verfügbarkeit **237**
12.1 Einleitung . . . 237
12.2 Denial-of-Service (DoS) . . . 239

12.2.1 Klassifikation . . . 239
12.2.2 Ausnutzen von Schwachstellen: Ping of Death . . . 240
12.2.3 Ausnutzen von Schwachstellen und Überlastung . . . 240
12.2.3.1 SYN-Flood . . . 240
12.2.3.2 Distributed-Denial-of-Service (DDos) . . . 243
12.2.4 Herbeiführen einer Überlastung . . . 244
12.2.4.1 Überlastsituationen . . . 244
12.2.4.2 TCP Überlastkontrolle . . . 244
12.2.4.3 Smurf-Angriff . . . 245
12.3 Zusammenfassung . . . 246
12.4 Übungsaufgaben . . . 246
12.4.1 Wiederholungsaufgaben . . . 246
12.4.2 Weiterführende Aufgaben . . . 247

13 Netzwerkanwendungen 249
13.1 Email . . . 249
13.1.1 Grundlegende Funktionsweise und Architektur von Email . . . 249
13.1.2 SMTP und POP – Eine kurze Darstellung aus Sicherheitsperspektive . . . 251
13.1.2.1 POP . . . 251
13.1.2.2 SMTP . . . 252
13.1.3 Email als Ende-zu-Ende-Anwendung . . . 253
13.1.3.1 Einführung . . . 253
13.1.3.2 S/MIME . . . 255
13.1.3.3 GPG . . . 256
13.2 SSH . . . 256
13.2.1 Einführung . . . 256
13.2.2 SSH Port Forwarding . . . 257
13.2.3 Praktisches Beispiel: Zugriff auf einen Server durch eine Firewall . . . 259
13.3 Das World Wide Web (WWW) . . . 262
13.3.1 Einführung . . . 262
13.3.2 HTTPS . . . 265
13.3.3 SSL und TLS . . . 266
13.3.4 Client-Authentifikation . . . 268
13.3.5 Server-Authentifikation . . . 269
13.3.6 Phishing und Pharming . . . 270
13.3.7 Weitere Bedrohungen der Sicherheit durch das WWW . . . 272
13.3.7.1 Client . . . 272
13.3.7.2 Server . . . 273
13.3.8 Anonymität, Privatsphäre und das WWW . . . 274
13.4 Zusammenfassung . . . 278
13.5 Übungsaufgaben . . . 279
13.5.1 Wiederholungsaufgaben . . . 279
13.5.2 Weiterführende Aufgaben . . . 280

14 Realzeitkommunikation **281**
14.1 Anforderungen, Prinzipien, Protokolle . . . 281
14.1.1 Einführung . . . 281
14.1.2 Medientransport . . . 282
14.1.3 Realtime Transport Protocol (RTP) . . . 283
14.1.4 Signalisierung . . . 284
14.1.5 Session Initiation Protocol . . . 284
14.2 Sicherheit von Realzeitkommunikationsanwendungen . . . 286
14.2.1 Bedrohungen . . . 286
14.2.2 Gegenwärtige Einsatzformen im institutionellen Umfeld . . . 288
14.2.3 Gegenwärtige Einsatzformen im privaten Umfeld . . . 290
14.3 Protokolle für sichere Realzeitkommunikation . . . 291
14.3.1 Sicherer Medientransport: SRTP . . . 291
14.3.2 Sicherheitsaspekte bei der Signalisierung . . . 293
14.3.3 SIP-Sicherheitsfunktionen . . . 295
14.4 Zusammenfassung . . . 296
14.5 Übungsaufgaben . . . 296
14.5.1 Wiederholungsaufgaben . . . 296
14.5.2 Weiterführende Aufgaben . . . 297

15 Sicherheit auf der Datenverbindungsschicht und in lokalen Netzen **299**
15.1 Das Extensible Authentication Protocol (EAP) . . . 299
15.1.1 Einführung . . . 299
15.1.2 Nachrichtenformat . . . 300
15.1.3 Architektur . . . 302
15.1.4 Einige EAP-Typen im Detail . . . 303
15.1.4.1 EAP-TLS . . . 303
15.1.4.2 EAP-TTLS und PEAP . . . 304
15.1.4.3 EAP-FAST . . . 304
15.2 Zugangskontrolle in LANs . . . 305
15.2.1 Einführung . . . 305
15.2.2 Ungesicherte lokale Netze . . . 305
15.2.3 IEEE 802.1X Port-based Access Control . . . 306
15.2.3.1 Funktionsweise . . . 306
15.2.3.2 Authentifikation . . . 308
15.3 Sicherheit in WLANs . . . 310
15.3.1 Eine kurze Einführung in IEEE 802.11 . . . 310
15.3.2 Sicherheit drahtloser LANs . . . 311
15.3.3 Schwachstellen im ursprünglichen IEEE 802.11-Standard . . . 312
15.3.4 IEEE 802.11i . . . 313
15.3.5 VPN-basierter Zugriff auf drahtlose LANs . . . 315
15.4 Zusammenfassung . . . 316
15.5 Übungsaufgaben . . . 317
15.5.1 Wiederholungsaufgaben . . . 317

15.5.2 Weiterführende Aufgaben 317

16 Richtlinien für die Praxis **319**
16.1 Einleitung 319
16.2 IT-Sicherheit im institutionellen Umfeld 319
16.2.1 Organisation und Administration 319
16.2.2 Leitlinien zur Erstellung und Beibehaltung sicherer IT-Strukturen 321
16.2.3 Minimalanforderungen 322
16.3 IT Sicherheit im privaten Umfeld 324
16.4 Ausblick 324
16.5 Zusammenfassung 325
16.6 Übungsaufgaben 326
16.6.1 Wiederholungsaufgaben 326
16.6.2 Weiterführende Aufgaben 326

Anhang **327**

A Weiterführende Literatur **329**

Literaturverzeichnis **331**

Sachverzeichnis **339**