

Inhaltsverzeichnis

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	12
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
1.7.6	Das leidige Thema Vorratsdatenspeicherung	16
1.8	Zusammenfassung	17
1.9	Übungsaufgaben	17
1.9.1	Wiederholungsaufgaben	17
1.9.2	Weiterführende Aufgaben	18
2	Kryptographische Prinzipien und Methoden	19
2.1	Grundlagen	19
2.1.1	Definition	19
2.1.2	Modell	20
2.2	Verschlüsselungsverfahren	22
2.2.1	Vom Klartext zum Chiffretext	22
2.2.2	Sicherheit von Verschlüsselungsverfahren	23
2.2.2.1	Kryptanalyse	23
2.2.2.2	Ein absolut sicheres Verfahren	25
2.3	Symmetrische Verfahren und Public-Key-Verfahren	27
2.3.1	Grundlagen	27
2.3.2	Symmetrische Verfahren	27
2.3.3	Public-Key-Verfahren	29

2.3.4	Hybride Verfahren	31
2.4	Betriebsarten	33
2.4.1	Electronic Code Book	33
2.4.2	Cipher Block Chaining	34
2.4.3	Cipher Feedback Mode und Output Feedback Mode	35
2.4.4	Counter Mode	37
2.5	Zusammenfassung	38
2.6	Übungsaufgaben	39
2.6.1	Wiederholungsaufgaben	39
2.6.2	Weiterführende Aufgaben	40
3	Authentifikation	41
3.1	Grundlagen	41
3.2	Mögliche Faktoren zur Authentifikation	42
3.3	Passwörter	43
3.3.1	Größe des Passwortraums	43
3.3.2	Sicherheit der Passwortspeicherung beim Anwender und im System	45
3.3.3	Sicherheit der Passworteingabe und Übertragung	47
3.3.4	Passwörter – Eine Sicherheitslücke?	48
3.4	Tokens und Smart-Cards	49
3.5	Biometrie	50
3.6	Kryptographische Methoden	52
3.6.1	Authentifikation von Benutzern und Maschinen	52
3.6.2	Digitale Signatur	54
3.6.3	Infrastrukturen zur Authentifikation	56
3.6.3.1	Zertifikate und Certificate Authorities	56
3.6.3.2	Zertifikate in der Praxis: X.509	59
3.6.3.3	Beispiel: X.509 Zertifikate mit OpenSSL selbst erstellen	61
3.6.3.4	Online Certificate Status Protocol und Extended Validation	66
3.6.3.5	Web of Trust	67
3.7	Zusammenfassung	68
3.8	Übungsaufgaben	68
3.8.1	Wiederholungsaufgaben	68
3.8.2	Weiterführende Aufgaben	70
4	Betriebssysteme und ihre Sicherheitsaufgaben	71
4.1	Aufgaben und Aufbau von Betriebssystemen	71
4.2	Systemadministratoren	73
4.3	Rechtevergabe und Zugriffskontrolle am Beispiel Dateisystem	74
4.4	Trusted Computing	79
4.5	Monitoring und Logging	80
4.6	Absichern des Systems gegen Angriffe	80
4.7	Zusammenfassung	81
4.8	Übungsaufgaben	82

4.8.1	Wiederholungsaufgaben	82
4.8.2	Weiterführende Aufgaben	82
5	Anwendungen	85
5.1	Einführung	85
5.2	Buffer Overflows	86
5.2.1	Das Problem	86
5.2.2	Schutzmaßnahmen	88
5.3	Race Conditions	88
5.4	Software aus dem Internet	90
5.4.1	Downloads	90
5.4.2	Aktive Inhalte	90
5.4.2.1	Einführung	90
5.4.2.2	Java und Java-Applets	91
5.4.2.3	JavaScript	93
5.4.2.4	ActiveX Control	93
5.5	Zusammenfassung	93
5.6	Übungsaufgaben	94
5.6.1	Wiederholungsaufgaben	94
5.6.2	Weiterführende Aufgaben	94
6	Malware	95
6.1	Einführung	95
6.2	Schaden	96
6.3	Verbreitung und Funktionsweise	97
6.3.1	Verbreitung	97
6.3.2	Funktionsweise	98
6.3.2.1	Viren	98
6.3.2.2	Würmer	99
6.3.2.3	Backdoors und Root Kits	100
6.3.2.4	Zombies	100
6.4	Schutzmaßnahmen und Entfernung von Malware	101
6.4.1	Schutzmaßnahmen	101
6.4.1.1	Virens Scanner	101
6.4.1.2	Systemkonfiguration, Dienste und Einstellungen	101
6.4.1.3	Patches und Updates	102
6.4.1.4	Heterogenität	102
6.4.1.5	Firewalls und Filtermechanismen	102
6.4.1.6	Vorsichtige Benutzer	103
6.4.2	Entfernung	103
6.5	Zusammenfassung	104
6.6	Übungsaufgaben	104
6.6.1	Wiederholungsaufgaben	104
6.6.2	Weiterführende Aufgaben	105

7	Netzwerke und Netzwerkprotokolle	107
7.1	Grundlagen	107
7.2	Das Schichtenmodell	108
7.3	Die wichtigsten Netzwerkprotokolle im Überblick	112
7.3.1	Datenverbindungsschicht: LAN-Technologien	112
7.3.1.1	IEEE 802.3 / Ethernet	112
7.3.1.2	IEEE 802.11 Wireless Local Area Networks	113
7.3.1.3	Bridges und Switches	113
7.3.2	Datenverbindungsschicht: Das Point-to-Point Protocol (PPP)	114
7.3.3	Netzwerkschicht: Internet Protocol (IP)	114
7.3.3.1	IP-Header	115
7.3.3.2	IPv4 und IPv6	116
7.3.3.3	Das ICMP-Protokoll	117
7.3.3.4	Routing unter IP	117
7.3.3.5	Automatische Konfiguration von Rechnern	119
7.3.3.6	An der Schnittstelle von IP und Datenverbindungsschicht: Address Resolution Protocol	119
7.3.4	Transportschicht: TCP und UDP	120
7.3.4.1	TCP	120
7.3.4.2	User Datagram Protocol (UDP)	125
7.3.4.3	Vergleich	125
7.3.5	Applikationsschicht	127
7.3.5.1	Ein kleiner Spaziergang durch den Zoo der Applikationsprotokolle	127
7.3.5.2	Domain Name Service (DNS)	127
7.4	Netzwerke in der Praxis	128
7.4.1	Referenznetzwerk	128
7.4.2	Konfiguration der Rechner und Router	130
7.4.3	Unser Test	134
7.4.4	Sniffer und Protokollanalysierer	137
7.5	Zusammenfassung	138
7.6	Übungsaufgaben	138
7.6.1	Wiederholungsaufgaben	138
7.6.2	Weiterführende Aufgaben	139
8	Sicherheit in Netzwerken	141
8.1	Bedrohungen	141
8.1.1	Bedrohungssituation	141
8.1.2	Struktur des Internet	142
8.1.3	Mithören in der Praxis	142
8.1.4	Manipulieren von Nachrichten	144
8.1.5	Schutzmechanismen	145
8.1.6	Anonymität	145
8.2	Beispiele für Schwachstellen und Risiken in Netzwerken und Netzwerkprotokollen	146

8.2.1	Manipulationen beim Routing	146
8.2.2	MAC-Address-Spoofing	147
8.2.3	ARP-Spoofing	147
8.2.4	IP-Spoofing	148
8.2.5	TCP Sequence Number Attack	149
8.2.6	DNS-Spoofing	151
8.3	Sicherheitsprotokolle im Internet – Ein Überblick	152
8.3.1	Sicherheit auf der Applikationsschicht	153
8.3.2	Sicherheit auf der Transportschicht	155
8.3.3	Sicherheit auf der Netzwerkschicht	156
8.3.4	Sicherheit auf der Daten Verbindungsschicht	158
8.4	Zusammenfassung	159
8.5	Übungsaufgaben	160
8.5.1	Wiederholungsaufgaben	160
8.5.2	Weiterführende Aufgaben	160
9	Firewalls	161
9.1	Der Grundgedanke von Firewalls	161
9.2	Komponenten von Firewalls	163
9.2.1	Paketfilter-Firewalls	163
9.2.1.1	Einführung	163
9.2.1.2	Typische Konfigurationen von Paketfiltern	164
9.2.1.3	Statische vs. dynamische Paketfilter	165
9.2.1.4	Probleme und Grenzen von Paketfiltern	169
9.2.1.5	Network Address Translation	171
9.2.1.6	Paketfilter unter Linux	175
9.2.2	Applikation-Level-Gateways	183
9.2.2.1	Einführung	183
9.2.3	Application-Level-Gateways und Paketfilter in der Praxis	186
9.3	Firewall-Architekturen	186
9.3.1	Einfache Firewall	186
9.3.2	Demilitarized Zone (DMZ)	187
9.4	Schwachstellen im Konzept von Firewalls	190
9.4.1	Einführung	190
9.4.2	Mobile Rechner	190
9.4.3	Tunnel und Verschlüsselung	191
9.5	Personal Firewalls	194
9.6	Zusammenfassung	194
9.7	Übungsaufgaben	195
9.7.1	Wiederholungsaufgaben	195
9.7.2	Weiterführende Aufgaben	196
10	Virtual Private Networks (VPN)	197
10.1	Einführung	197

10.2 Technische Realisierung eines Remote-Access-VPNs	199
10.3 VPNs als Ersatz dedizierter Datenleitungen	201
10.4 IPsec	202
10.4.1 Einführung	202
10.4.2 Das AH-Protokoll	204
10.4.3 Das ESP-Protokoll	206
10.4.4 Aufbau und Verwaltung von SAs und Schlüsselmanagement	209
10.4.5 Praktisches Beispiel	212
10.5 OpenVPN	215
10.5.1 Einführung	215
10.5.2 Praktisches Beispiel	217
10.6 VPN-Technologien und Klassifikation	221
10.7 Risiken bei der Verwendung von VPNs	223
10.7.1 Split Tunneling	223
10.7.2 Öffentliche Zugangsnetze für Endsysteme	224
10.8 Zusammenfassung	226
10.9 Übungsaufgaben	227
10.9.1 Wiederholungsaufgaben	227
10.9.2 Weiterführende Aufgaben	227
11 Netzwerküberwachung	229
11.1 Grundlagen	229
11.2 Intrusion Detection	230
11.2.1 Einführung	230
11.2.2 Architektur und Komponenten eines netzwerkbasierten IDS	232
11.2.3 Netzwerkbasierte IDS und Paketfilter	234
11.2.4 Beispiel für die Verwendung eines IDS	235
11.3 Scannen	237
11.3.1 Einführung	237
11.3.2 Finden von Geräten im Netz	238
11.3.2.1 Ping-Sweep	238
11.3.2.2 Address Resolution Protocol	239
11.3.2.3 Domain Name Service	240
11.3.3 Portscanning	240
11.3.3.1 Prinzipielle Vorgehensweise	240
11.3.3.2 TCP-Connect-Scan	240
11.3.3.3 TCP-SYN-Scan	241
11.3.3.4 Weitere TCP-Scans	242
11.3.3.5 OS-Fingerprinting	243
11.3.4 Schutz vor Scanning	243
11.3.5 Scanning zum Schutz des Netzes	244
11.4 Zusammenfassung	245
11.5 Übungsaufgaben	246
11.5.1 Wiederholungsaufgaben	246

11.5.2 Weiterführende Aufgaben	246
12 Verfügbarkeit	247
12.1 Einleitung	247
12.2 Denial-of-Service (DoS)	249
12.2.1 Klassifikation	249
12.2.2 Ausnutzen von Schwachstellen: Ping of Death	250
12.2.3 Ausnutzen von Schwachstellen und Überlastung	250
12.2.3.1 SYN-Flood	250
12.2.3.2 Distributed-Denial-of-Service (DDoS)	253
12.2.4 Herbeiführen einer Überlastung	254
12.2.4.1 Überlastsituationen	254
12.2.4.2 TCP Überlastkontrolle	254
12.2.4.3 Smurf-Angriff	255
12.3 Zusammenfassung	256
12.4 Übungsaufgaben	256
12.4.1 Wiederholungsaufgaben	256
12.4.2 Weiterführende Aufgaben	257
13 Netzerkanwendungen	259
13.1 Email	259
13.1.1 Grundlegende Funktionsweise und Architektur von Email	259
13.1.2 SMTP und POP – Eine kurze Darstellung aus Sicherheitsperspektive	261
13.1.2.1 POP	261
13.1.2.2 SMTP	262
13.1.3 Email als Ende-zu-Ende-Anwendung	263
13.1.3.1 Einführung	263
13.1.3.2 S/MIME	265
13.1.3.3 OpenPGP	266
13.2 SSH	266
13.2.1 Einführung	266
13.2.2 SSH Port Forwarding	267
13.2.3 Praktisches Beispiel: Zugriff auf einen Server durch eine Firewall	269
13.3 Das World Wide Web (WWW)	272
13.3.1 Einführung	272
13.3.2 HTTPS	275
13.3.3 SSL und TLS	276
13.3.3.1 Aufbau	276
13.3.3.2 SSL/TLS Handshake Protocol	278
13.3.4 Client-Authentifikation	280
13.3.5 Server-Authentifikation	281
13.3.6 Praktischer Test von SSL/TLS mit Java	282
13.3.7 Phishing und Pharming	286
13.3.8 Weitere Bedrohungen der Sicherheit durch das WWW	288

13.3.8.1	Client	288
13.3.8.2	Server	289
13.3.9	Anonymität, Privatsphäre und das WWW	290
13.4	Zusammenfassung	294
13.5	Übungsaufgaben	295
13.5.1	Wiederholungsaufgaben	295
13.5.2	Weiterführende Aufgaben	296
14	Realzeitkommunikation	297
14.1	Anforderungen, Prinzipien, Protokolle	297
14.1.1	Einführung	297
14.1.2	Medientransport	298
14.1.3	Realtime Transport Protocol (RTP)	299
14.1.4	Signalisierung	300
14.1.5	Session Initiation Protocol	300
14.2	Sicherheit von Realzeitkommunikationsanwendungen	302
14.2.1	Bedrohungen	302
14.2.2	Gegenwärtige Einsatzformen im institutionellen Umfeld	304
14.2.3	Gegenwärtige Einsatzformen im privaten Umfeld	306
14.3	Protokolle für sichere Realzeitkommunikation	308
14.3.1	Sicherer Medientransport: SRTP	308
14.3.2	Sicherheitsaspekte bei der Signalisierung	310
14.3.3	SIP-Sicherheitsfunktionen	311
14.4	Zusammenfassung	312
14.5	Übungsaufgaben	312
14.5.1	Wiederholungsaufgaben	312
14.5.2	Weiterführende Aufgaben	313
15	Sicherheit auf der Datenverbindungsschicht und in lokalen Netzen	315
15.1	Das Extensible Authentication Protocol (EAP)	315
15.1.1	Einführung	315
15.1.2	Nachrichtenformat	316
15.1.3	Architektur	318
15.1.4	Einige EAP-Typen im Detail	319
15.1.4.1	EAP-TLS	319
15.1.4.2	EAP-TTLS und PEAP	320
15.1.4.3	EAP-FAST	320
15.2	Zugangskontrolle in LANs	321
15.2.1	Einführung	321
15.2.2	Ungesicherte lokale Netze	321
15.2.3	IEEE 802.1X Port-based Access Control	322
15.2.3.1	Funktionsweise	322
15.2.3.2	Authentifikation	324
15.3	Sicherheit in WLANs	325

15.3.1	Eine kurze Einführung in IEEE 802.11	325
15.3.2	Sicherheit drahtloser LANs	326
15.3.3	Schwachstellen im ursprünglichen IEEE 802.11-Standard	328
15.3.4	Der aktuelle IEEE 802.11-Standard	329
15.3.5	VPN-basierter Zugriff auf drahtlose LANs	331
15.4	Zusammenfassung	332
15.5	Übungsaufgaben	333
15.5.1	Wiederholungsaufgaben	333
15.5.2	Weiterführende Aufgaben	333
16	Richtlinien für die Praxis	335
16.1	Einleitung	335
16.2	IT-Sicherheit im institutionellen Umfeld	335
16.2.1	Organisation und Administration	335
16.2.2	Leitlinien zur Erstellung und Beibehaltung sicherer IT-Strukturen	337
16.2.3	Minimalanforderungen	338
16.3	IT-Sicherheit im privaten Umfeld	340
16.4	Ausblick	340
16.5	Zusammenfassung	341
16.6	Übungsaufgaben	342
16.6.1	Wiederholungsaufgaben	342
16.6.2	Weiterführende Aufgaben	342
Literaturverzeichnis		343
Klassische Referenzen		343
Online-Referenzen		350
Weiterführende Literatur		351
Sachverzeichnis		353