

Inhaltsverzeichnis

1	Einführung	1
1.1	Warum IT-Sicherheit	1
1.2	Ziele von IT-Sicherheit	3
1.3	Angriffe auf IT-Sicherheit	6
1.3.1	Angriffsarten	6
1.3.2	Schwachstellen	7
1.3.3	Ziele eines Angriffs	8
1.4	Risiken und Unsicherheit	9
1.5	IT-Sicherheit in der Praxis	11
1.6	Organisatorische Grundlagen der IT-Sicherheit	12
1.6.1	Rahmenbedingungen	12
1.6.2	IT-Sicherheit als Prozess	12
1.7	Rechtliche Grundlagen und Rahmenbedingungen in Deutschland	13
1.7.1	Strafgesetzbuch	14
1.7.2	Datenschutzgrundverordnung	14
1.7.3	Telekommunikation-Telemedien-Datenschutz-Gesetz	15
1.7.4	Handelsgesetzbuch	16
1.7.5	Bundesamt für Sicherheit in der Informationstechnik	16
1.7.6	Vorratsdatenspeicherung	19
1.8	Zusammenfassung	20
1.9	Übungsaufgaben	21
1.9.1	Wiederholungsaufgaben	21
1.9.2	Weiterführende Aufgaben	22
	Literatur	22
2	Kryptographische Prinzipien und Methoden	25
2.1	Grundlagen	25
2.1.1	Definition	25
2.1.2	Modell	26

2.2	Verschlüsselungsverfahren	28
2.2.1	Vom Klartext zum Chiffretext	28
2.2.2	Sicherheit von Verschlüsselungsverfahren	30
2.2.2.1	Kryptanalyse	30
2.2.2.2	Ein absolut sicheres Verfahren	32
2.3	Symmetrische Verfahren und Public-Key-Verfahren	34
2.3.1	Grundlagen	34
2.3.2	Symmetrische Verfahren	35
2.3.3	Public-Key-Verfahren	36
2.3.4	Hybride Verfahren	38
2.4	Betriebsarten	40
2.4.1	Electronic Code Book	40
2.4.2	Cipher Block Chaining	41
2.4.3	Cipher Feedback Mode und Output Feedback Mode	42
2.4.4	Counter Mode	43
2.5	Zusammenfassung	45
2.6	Übungsaufgaben	47
2.6.1	Wiederholungsaufgaben	47
2.6.2	Weiterführende Aufgaben	48
	Literatur	50
3	Authentifikation	51
3.1	Grundlagen	51
3.2	Mögliche Faktoren zur Authentifikation	52
3.3	Passwörter	53
3.3.1	Größe des Passwortsraums	54
3.3.2	Sicherheit der Passwortspeicherung beim Anwender und im System	55
3.3.3	Sicherheit der Passworteingabe und Übertragung	58
3.3.4	Passwörter – Eine Sicherheitslücke?	59
3.4	Tokens und Smart-Cards	60
3.5	Biometrie	62
3.6	Kryptographische Methoden	63
3.6.1	Authentifikation von Benutzern und Maschinen	63
3.6.2	Digitale Signatur	66
3.6.3	Infrastrukturen zur Authentifikation	68
3.6.3.1	Zertifikate und Certificate Authorities	68
3.6.3.2	Zertifikate in der Praxis: X.509	72
3.6.3.3	Beispiel: X.509 Zertifikate mit OpenSSL selbst erstellen	74
3.6.3.4	Online Certificate Status Protocol und Extended Validation	79
3.6.3.5	Web of Trust	80

3.7	Zusammenfassung	81
3.8	Übungsaufgaben.....	81
3.8.1	Wiederholungsaufgaben.....	81
3.8.2	Weiterführende Aufgaben	83
	Literatur.....	84
4	Betriebssysteme und ihre Sicherheitsaufgaben	85
4.1	Aufgaben und Aufbau von Betriebssystemen	85
4.2	Systemadministratoren.....	87
4.3	Rechtevergabe und Zugriffskontrolle am Beispiel Dateisystem	88
4.4	Trusted Computing.....	95
4.5	Monitoring und Logging	95
4.6	Absichern des Systems gegen Angriffe	96
4.7	Zusammenfassung	97
4.8	Übungsaufgaben.....	98
4.8.1	Wiederholungsaufgaben.....	98
4.8.2	Weiterführende Aufgaben	98
	Literatur.....	99
5	Anwendungen	101
5.1	Einführung	101
5.2	Buffer Overflows	102
5.2.1	Das Problem.....	102
5.2.2	Beispiel.....	105
5.2.3	Schutzmaßnahmen	106
5.3	Race Conditions	107
5.4	Software aus dem Internet	109
5.4.1	Downloads	109
5.4.2	Aktive Inhalte.....	110
5.4.2.1	Einführung.....	110
5.4.2.2	Java	110
5.4.2.3	JavaScript	112
5.5	Zusammenfassung	113
5.6	Übungsaufgaben.....	114
5.6.1	Wiederholungsaufgaben.....	114
5.6.2	Weiterführende Aufgaben	114
	Literatur.....	114
6	Malware	115
6.1	Einführung	115
6.2	Schaden	116
6.3	Verbreitung und Funktionsweise	117
6.3.1	Verbreitung.....	117

6.3.2	Funktionsweise.	118
6.3.2.1	Viren	118
6.3.2.2	Würmer	120
6.3.2.3	Backdoors und Root Kits	120
6.3.2.4	Bots	121
6.4	Schutzmaßnahmen und Entfernung von Malware	121
6.4.1	Schutzmaßnahmen	121
6.4.1.1	Virens Scanner	121
6.4.1.2	Systemkonfiguration, Dienste und Einstellungen.	122
6.4.1.3	Patches und Updates	123
6.4.1.4	Heterogenität.	123
6.4.1.5	Firewalls und Filtermechanismen	123
6.4.1.6	Vorsichtige Benutzer	124
6.4.2	Entfernung	124
6.5	Zusammenfassung	125
6.6	Übungsaufgaben.	126
6.6.1	Wiederholungsaufgaben.	126
6.6.2	Weiterführende Aufgaben	126
7	Netzwerke und Netzwerkprotokolle	127
7.1	Grundlagen.	127
7.2	Das Schichtenmodell	128
7.3	Die wichtigsten Netzwerkprotokolle im Überblick	132
7.3.1	Datenverbindungsschicht: LAN-Technologien	132
7.3.1.1	IEEE 802.3/Ethernet	132
7.3.1.2	IEEE 802.11 Wireless Local Area Networks	134
7.3.1.3	Bridges und Switches	134
7.3.2	Datenverbindungsschicht: Das Point-to-Point Protocol (PPP)	134
7.3.3	Netzwerkschicht: Internet Protocol (IP).	135
7.3.3.1	IPv4-Header	136
7.3.3.2	IPv6-Header	137
7.3.3.3	ICMP und ICMPv6-Protokoll.	138
7.3.3.4	Routing unter IPv4	139
7.3.3.5	Routing unter IPv6	142
7.3.3.6	Automatische Konfiguration von Rechnern	142
7.3.3.7	An der Schnittstelle von IP und Datenverbindungsschicht: Address Resolution Protocol und Neighbor Discovery Protocol	143
7.3.3.8	Dual Stack	143

7.3.4	Transportschicht: TCP und UDP	144
7.3.4.1	Transmission Control Protocol (TCP)	144
7.3.4.2	User Datagram Protocol (UDP)	149
7.3.4.3	Vergleich	150
7.3.5	Applikationsschicht	151
7.3.5.1	Ein kleiner Spaziergang durch den Zoo der Applikationsprotokolle	151
7.3.5.2	Domain Name Service (DNS)	151
7.4	Netzwerke in der Praxis	153
7.4.1	Referenznetzwerk	153
7.4.2	Konfiguration der Rechner und Router	154
7.4.3	Unser Test	159
7.4.4	Sniffer und Protokollanalysierer	161
7.4.5	Referenznetzwerk für IPv6	163
7.5	Zusammenfassung	167
7.6	Übungsaufgaben	168
7.6.1	Wiederholungsaufgaben	168
7.6.2	Weiterführende Aufgaben	169
	Literatur	169
8	Sicherheit in Netzwerken	173
8.1	Bedrohungen	173
8.1.1	Bedrohungssituation	173
8.1.2	Struktur des Internet	174
8.1.3	Mithören in der Praxis	175
8.1.4	Manipulieren von Nachrichten	176
8.1.5	Schutzmechanismen	177
8.1.6	Anonymität	178
8.2	Beispiele für Schwachstellen und Risiken in Netzwerken und Netzwerkprotokollen	178
8.2.1	Manipulationen beim Routing	178
8.2.2	MAC-Address-Spoofing	179
8.2.3	ARP-Spoofing	180
8.2.4	IP-Spoofing	181
8.2.5	TCP Sequence Number Attack	182
8.2.6	Pharming	184
8.3	Sicherheitsprotokolle im Internet – Ein Überblick	185
8.3.1	Sicherheit auf der Applikationsschicht	186
8.3.2	Sicherheit auf der Transportschicht	188
8.3.3	Sicherheit auf der Netzwerkschicht	190
8.3.4	Sicherheit auf der Datenverbindungsschicht	191
8.4	Zusammenfassung	193

8.5	Übungsaufgaben.	193
8.5.1	Wiederholungsaufgaben.	193
8.5.2	Weiterführende Aufgaben	194
	Literatur.	194
9	Firewalls.	195
9.1	Der Grundgedanke von Firewalls.	195
9.2	Komponenten von Firewalls.	198
9.2.1	Paketfilter-Firewalls	198
9.2.1.1	Einführung.	198
9.2.1.2	Typische Konfigurationen von Paketfiltern.	199
9.2.1.3	Statische vs. dynamische Paketfilter	200
9.2.1.4	Probleme und Grenzen von Paketfiltern	205
9.2.1.5	Network Address Translation	206
9.2.1.6	IPv4-Paketfilter unter Linux	210
9.2.1.7	IPv6-Paketfilter unter Linux	219
9.2.2	Applikation-Level-Gateways	220
9.2.2.1	Einführung.	220
9.2.3	Application-Level-Gateways und Paketfilter in der Praxis	223
9.3	Firewall-Architekturen.	223
9.3.1	Einfache Firewall	223
9.3.2	Demilitarized Zone (DMZ)	225
9.4	Schwachstellen im Konzept von Firewalls.	227
9.4.1	Einführung	227
9.4.2	Mobile Rechner	228
9.4.3	Tunnel und Verschlüsselung.	228
9.5	Personal Firewalls	232
9.6	Zusammenfassung	233
9.7	Übungsaufgaben.	233
9.7.1	Wiederholungsaufgaben.	233
9.7.2	Weiterführende Aufgaben	234
	Literatur.	236
10	Virtual Private Networks (VPN)	237
10.1	Einführung	237
10.2	Technische Realisierung eines Remote-Access-VPNs	239
10.3	VPNs als Ersatz dedizierter Datenleitungen	240
10.4	IPsec.	242
10.4.1	Einführung	242
10.4.2	Das AH-Protokoll.	245
10.4.3	Das ESP-Protokoll	246
10.4.4	Aufbau und Verwaltung von SAs und Schlüsselmanagement	249
10.4.5	Praktisches Beispiel	253

10.5	OpenVPN	256
10.5.1	Einführung	256
10.5.2	Praktisches Beispiel	257
10.6	VPN-Technologien und Klassifikation	261
10.7	Risiken bei der Verwendung von VPNs	263
10.7.1	Split Tunneling	263
10.7.2	Öffentliche Zugangsnetze für Endsysteme	265
10.8	Zusammenfassung	267
10.9	Übungsaufgaben	267
10.9.1	Wiederholungsaufgaben	267
10.9.2	Weiterführende Aufgaben	268
	Literatur	269
11	Netzwerküberwachung	271
11.1	Grundlagen	271
11.2	Intrusion Detection	272
11.2.1	Einführung	272
11.2.2	Anomalieerkennungsverfahren	273
11.2.3	Architektur und Komponenten eines netzwerkbasierten IDS	274
11.2.4	Netzwerkbasierte IDS und Paketfilter	277
11.2.5	Beispiel für die Verwendung eines IDS	278
11.3	Scannen	281
11.3.1	Einführung	281
11.3.2	Finden von Geräten im Netz	281
11.3.2.1	Ping-Sweep	281
11.3.2.2	Address Resolution Protocol	283
11.3.2.3	Domain Name Service	283
11.3.3	Portscanning	284
11.3.3.1	Prinzipielle Vorgehensweise	284
11.3.3.2	TCP-Connect-Scan	284
11.3.3.3	TCP-SYN-Scan	285
11.3.3.4	Weitere TCP-Scans	286
11.3.3.5	OS-Fingerprinting	287
11.3.4	Schutz vor Scanning	287
11.3.5	Scanning zum Schutz des Netzes	288
11.4	Zusammenfassung	289
11.5	Übungsaufgaben	290
11.5.1	Wiederholungsaufgaben	290
11.5.2	Weiterführende Aufgaben	291
	Literatur	291

12 Verfügbarkeit	293
12.1 Einleitung	293
12.2 Denial-of-Service (DoS)	295
12.2.1 Klassifikation	295
12.2.2 Ausnutzen von Schwachstellen: Ping of Death	296
12.2.3 Ausnutzen von Schwachstellen und Überlastung	297
12.2.3.1 SYN-Flood	297
12.2.3.2 Distributed-Denial-of-Service (DDoS)	300
12.2.4 Herbeiführen einer Überlastung	300
12.2.4.1 Überlastsituationen	300
12.2.4.2 TCP Überlastkontrolle	301
12.2.4.3 Smurf-Angriff	302
12.3 Zusammenfassung	303
12.4 Übungsaufgaben	303
12.4.1 Wiederholungsaufgaben	303
12.4.2 Weiterführende Aufgaben	304
Literatur	304
13 Netzwerkanwendungen	305
13.1 Email	305
13.1.1 Grundlegende Funktionsweise und Architektur von Email	305
13.1.2 SMTP und POP – Eine kurze Darstellung aus Sicherheitsperspektive	307
13.1.2.1 POP	307
13.1.2.2 SMTP	309
13.1.3 Email als Ende-zu-Ende-Anwendung	310
13.1.3.1 Einführung	310
13.1.3.2 S/MIME	312
13.1.3.3 OpenPGP	312
13.2 SSH	313
13.2.1 Einführung	313
13.2.2 SSH Port Forwarding	314
13.2.3 Praktisches Beispiel: Zugriff auf einen Server durch eine Firewall	316
13.3 Das Web	320
13.3.1 Einführung	320
13.3.2 HTTPS	322
13.3.3 TLS	323
13.3.3.1 Aufbau	323
13.3.3.2 TLS Handshake Protocol	325

13.3.4	Client-Authentifikation	327
13.3.5	Server-Authentifikation	328
13.3.6	Praktischer Test von TLS mit Java	331
13.3.7	Phishing	334
13.3.8	Anonymität, Privatsphäre und das Web	336
13.4	Zusammenfassung	341
13.5	Übungsaufgaben	342
13.5.1	Wiederholungsaufgaben	342
13.5.2	Weiterführende Aufgaben	342
	Literatur	344
14	Webanwendungen	347
14.1	Einleitung	347
14.1.1	Grundlegende Funktionsweise von Webanwendungen	347
14.1.2	Sicherheitsaspekte	348
14.1.2.1	Clientsicherheit	348
14.1.2.2	Backendsicherheit	350
14.1.2.3	Sicherheit des Datenaustauschs und von gespeicherten Daten	351
14.1.2.4	Sicherheit der Webanwendung selbst	351
14.2	Injection	352
14.2.1	Das grundlegende Problem	352
14.2.2	Command Injection	352
14.2.3	SQL Injection	355
14.2.4	Schutzmaßnahmen	357
14.3	Cross-Site Scripting (XSS)	358
14.3.1	Das grundlegende Problem	358
14.3.2	Stored XSS	358
14.3.3	Reflected XSS	360
14.3.4	Client-basierte XSS	362
14.3.5	Schutzmaßnahmen	362
14.4	Cross-Site Request Forgery (CSRF)	363
14.4.1	Das grundlegende Problem	363
14.4.2	Schutzmaßnahmen	364
14.5	OWASP Top 10	364
14.6	Zusammenfassung	365
14.7	Übungsaufgaben	366
14.7.1	Wiederholungsaufgaben	366
14.7.2	Weiterführende Aufgaben	366
	Literatur	367

15 Cloud Computing	369
15.1 Grundlagen des Cloud Computing	369
15.1.1 Einführung	369
15.1.2 Technologien zum Ermöglichen von Cloud Computing	370
15.1.2.1 Virtualisierung	370
15.1.2.2 Transparente Verteilung	371
15.1.3 Bereitstellungsmodelle	372
15.1.3.1 Private Cloud	372
15.1.3.2 Public Cloud	372
15.1.3.3 Mischformen	372
15.1.4 Dienste	372
15.1.4.1 Infrastructure as a Service (IaaS)	372
15.1.4.2 Platform as a Service (PaaS)	373
15.1.4.3 Software as a Service (SaaS)	373
15.2 Sicherheitsaspekte	373
15.2.1 Einführung	373
15.2.2 Sicherheit des Anwendersystems	374
15.2.3 Sicherheit der Netzwerkverbindung	374
15.2.4 Sicherheit des Hostsystems und der Abstraktionsebene	375
15.2.5 Sicherheit des Gastes	375
15.2.6 Weitere Überlegungen	376
15.3 Zusammenfassung	376
15.4 Übungsaufgaben	377
15.4.1 Wiederholungsaufgaben	377
15.4.2 Weiterführende Aufgaben	377
Literatur	377
16 Realzeitkommunikation	379
16.1 Anforderungen, Prinzipien, Protokolle	379
16.1.1 Einführung	379
16.1.2 Medientransport	380
16.1.3 Realtime Transport Protocol (RTP)	381
16.1.4 Signalisierung	382
16.1.5 Session Initiation Protocol	383
16.2 Sicherheit von Realzeitkommunikationsanwendungen	386
16.2.1 Bedrohungen	386
16.2.2 Gegenwärtige Einsatzformen im institutionellen Umfeld	387
16.2.3 Gegenwärtige Einsatzformen im privaten Umfeld	389
16.3 Protokolle für sichere Realzeitkommunikation	390
16.3.1 Sicherer Medientransport: SRTP	390
16.3.2 Sicherheitsaspekte bei der Signalisierung	392
16.3.3 SIP-Sicherheitsfunktionen	394

16.4	Zusammenfassung	394
16.5	Übungsaufgaben.....	395
16.5.1	Wiederholungsaufgaben.....	395
16.5.2	Weiterführende Aufgaben	395
	Literatur.....	396
17	Sicherheit auf der Daten Verbindungsschicht und in lokalen Netzen	397
17.1	Das Extensible Authentication Protocol (EAP)	397
17.1.1	Einführung	397
17.1.2	Nachrichtenformat	398
17.1.3	Architektur	400
17.1.4	Einige EAP-Typen im Detail	401
17.1.4.1	EAP-TLS	401
17.1.4.2	EAP-TTLS und PEAP	402
17.1.4.3	EAP-FAST	403
17.2	Zugangskontrolle in LANs	403
17.2.1	Einführung	403
17.2.2	Ungesicherte lokale Netze	404
17.2.3	IEEE 802.1X Port-based Access Control	404
17.2.3.1	Funktionsweise	404
17.2.3.2	Authentifikation	407
17.3	Sicherheit in WLANs	408
17.3.1	Eine kurze Einführung in IEEE 802.11	408
17.3.2	Sicherheit drahtloser LANs	409
17.3.3	Schwachstellen im ursprünglichen IEEE 802.11-Standard	410
17.3.4	WPA und WPA2	412
17.3.5	WPA3	414
17.3.6	VPN-basierter Zugriff auf drahtlose LANs	414
17.4	Zusammenfassung	415
17.5	Übungsaufgaben.....	416
17.5.1	Wiederholungsaufgaben.....	416
17.5.2	Weiterführende Aufgaben	417
	Literatur.....	418
18	Richtlinien für die Praxis	419
18.1	Einleitung	419
18.2	IT-Sicherheit im institutionellen Umfeld	420
18.2.1	Organisation und Administration	420
18.2.2	Leitlinien zur Erstellung und Beibehaltung sicherer IT-Strukturen	421
18.2.3	Minimalanforderungen	422
18.3	IT Sicherheit im privaten Umfeld	424
18.4	Ausblick	425

18.5	Zusammenfassung	426
18.6	Übungsaufgaben.	427
18.6.1	Wiederholungsaufgaben.	427
18.6.2	Weiterführende Aufgaben	427
	Literatur.	427
	Literatur.	429
	Stichwortverzeichnis.	431