

1	Einleitung/Motivation	1
1.1	Was ist eigentlich ein Hacker?	3
1.2	Angriffe auf Rechnersysteme	6
1.3	Aufgaben & Lösungen zu diesem Kapitel	11
1.3.1	Aufgaben	11
1.3.2	Lösungen	12
	Literatur	13

Teil I Technische Grundlagen

2	Grundlagen	17
2.1	Betriebssysteme	17
2.2	Schichtenmodelle	19
2.3	MAC-Adressen	21
2.4	IP-Adressen	21
2.5	Die Protokolle TCP und UDP	24
2.6	IP-Ports	24
2.7	Network Address Translation	26
2.8	Das Tor-Netzwerk	27
2.9	Aufgaben & Lösungen zu diesem Kapitel	29
2.9.1	Aufgaben	29
2.9.2	Lösungen	30
	Literatur	32
3	Die Mechanismen verschiedener Arten von Schadsoftware	33
3.1	Trojaner	34
3.2	Viren	36
3.3	Backdoor	36
3.4	Computerwurm	37
3.5	Rootkit	37
3.6	Spyware	38

3.7	Adware	39
3.8	Ransomware	39
3.9	Botnet	39
3.10	Schutz durch Virens Scanner	40
3.11	Aufgaben & Lösungen zu diesem Kapitel	41
3.11.1	Aufgaben	41
3.11.2	Lösungen	42
	Literatur	43

Teil II Cyberangriffe

4	Angriffsmechanismen	47
4.1	Informationen sammeln	51
4.1.1	Footprinting	51
4.1.2	OS-Fingerprinting und Banner-Grabbing	53
4.2	Zugang erlangen	54
4.2.1	Phishing	54
4.2.2	Scanning-Techniken	56
4.2.3	Werkzeuge zum Scannen von Netzwerken	61
4.2.4	Maßnahmen gegen Scanning-Versuche	62
4.2.5	Firewalls umgehen	63
4.2.6	Angriffe auf Webserver	68
4.2.7	SQL-Injection (SQLi)	69
4.2.8	Cross-Site-Scripting (XSS)	73
4.2.9	Man-in-the-Middle-Angriffe	75
4.2.10	Passwortschutz aushebeln	77
4.2.11	Einsatz von Metasploit	81
4.3	Ausbreitung im Netzwerk und Erweiterung der Rechte	82
4.3.1	Lateral Movement	82
4.3.2	Privilege Escalation	84
4.4	Schadfunktion einrichten	85
4.5	Dateien verstecken	87
4.6	Spuren verwischen	88
4.7	Denial-of-Service-Attacken	90
4.8	Typischer Ablauf am Beispiel eines Ransomware-Cyberangriffs	93
4.9	Aufgaben & Lösungen zu diesem Kapitel	95
4.9.1	Aufgaben	95
4.9.2	Lösungen	100
	Literatur	102
5	Wireless Hacking	105
5.1	Privates, dienstliches und öffentliches WLAN	106
5.2	Betrieb eines öffentlichen WLAN	109

5.3	Wired Equivalent Privacy (WEP)	110
5.4	Wifi Protected Access (WPA)	111
5.5	Wifi Protected Access 2 (WPA2)	112
5.6	Wifi Protected Access 3 (WPA3)	113
5.7	Aufgaben & Lösungen zu diesem Kapitel	113
5.7.1	Aufgaben	113
5.7.2	Lösungen	114
	Literatur	115
6	Mobile Hacking	117
6.1	Besondere Gefahren bei mobilen Endgeräten	117
6.2	Spyware	119
6.3	Sicherungsmaßnahmen bei Android und iOS	120
6.3.1	Android	121
6.3.2	iOS und iPadOS	122
6.4	Aufgaben & Lösungen zu diesem Kapitel	123
6.4.1	Aufgaben	123
6.4.2	Lösungen	123
	Literatur	124
7	Internet of Things	125
7.1	Besondere Gefahren von IoT-Geräten	125
7.2	IoT-Kleingeräte	128
7.3	IoT-Großgeräte	129
7.4	Industrielle Produktionslagen	130
7.5	Aufgaben & Lösungen zu diesem Kapitel	131
7.5.1	Aufgaben	131
7.5.2	Lösungen	132
	Literatur	133
 Teil III Abwehr von Cyberattacken		
8	Allgemeine Maßnahmen	137
8.1	Umgang mit Passwörtern	139
8.2	Kampagnen zur Verbesserung der Phishing-Awareness	141
8.3	Zwei- oder Multifaktorauthentisierung (2FA und MFA)	144
8.4	Fast Identity Online (FIDO)	147
8.5	Web Authentication (WebAuthn)	150
8.6	Transport Layer Security (TLS)	152
8.7	Virtual Private Network (VPN)	155
8.8	Zero Trust als Netzwerksicherheitsmodell	156
8.9	Zero Trust Network Access (ZTNA)	161
8.10	Secure Access Service Edge (SASE)	163

8.11	Aufgaben & Lösungen zu diesem Kapitel	164
8.11.1	Aufgaben	164
8.11.2	Lösungen	167
	Literatur	168
9	Vorbereitungen für den Ernstfall	171
9.1	Awareness-Schulungen.	172
9.2	Common Vulnerabilities and Exposures (CVE) und das Common Vulnerability Scoring System (CVSS)	174
9.3	Die Wissensdatenbank MITRE ATT&CK	176
9.4	BSI IT-Grundschutz	177
9.5	Information-Security-Management-System (ISMS)	178
9.6	IT-Sicherheitstests und Notfallübungen	179
9.7	Aufgaben & Lösungen zu diesem Kapitel	180
9.7.1	Aufgaben	180
9.7.2	Lösungen	181
	Literatur	182
10	Penetration Tests	183
10.1	Auftragsklärung für einen Pentest	184
10.2	Arten von Pentests und Vulnerability-Scans	184
10.3	Social Engineering Pentests	186
10.4	Sicherheit von Web-Applikationen	187
10.5	Sicherheit von Arbeitsplatzrechnern	188
10.6	Schwachstellensuche in Netzwerken	189
10.6.1	Der Einsatz von Nmap	190
10.6.2	Greenbone Vulnerability Management (GVM)	195
10.7	Die Durchführung von Pentests	197
10.8	IT-Sicherheitsaudits	199
10.9	Aufgaben & Lösungen zu diesem Kapitel	201
10.9.1	Aufgaben	201
10.9.2	Lösungen	204
	Literatur	206
11	Intrusion Detection	209
11.1	Erkennen von Angriffen	209
11.2	Indicators of Compromise (IoC) und Indicators of Attack (IoA).	211
11.3	Intrusion Detection System (IDS)	213
11.4	Intrusion Prevention System (IPS)	215
11.5	Beispiele für Open-Source Intrusion-Detection-Systeme	216
11.5.1	Snort.	216
11.5.2	Suricata.	217
11.5.3	Zeek	217

11.6	Security Information and Event Management (SIEM)	218
11.7	Honeypots.....	219
11.8	Aufgaben & Lösungen zu diesem Kapitel	221
11.8.1	Aufgaben	221
11.8.2	Lösungen	222
	Literatur.....	223
12	Incident Response	225
12.1	IT-Security-Incidents	227
12.2	Sofortmaßnahmen im Falle eines Angriffs.....	229
12.3	Klassifizierung eines Security-Incidents	230
12.4	Der Incident-Response-Prozess	231
12.5	Aufgaben & Lösungen zu diesem Kapitel	234
12.5.1	Aufgaben	234
12.5.2	Lösungen	235
	Literatur.....	236
13	IT-Forensik	237
13.1	Sicherungsphase.....	238
13.1.1	Persistente Daten	239
13.1.2	Volatile Daten.....	241
13.2	Analysephase	241
13.3	Präsentationsphase	244
13.4	Abschließende Bemerkungen zur IT-Forensik.....	245
13.5	Aufgaben & Lösungen zu diesem Kapitel	246
13.5.1	Aufgaben	246
13.5.2	Lösungen	247
	Literatur.....	249
14	Fallbeispiele erfolgreicher Angriffe	251
14.1	Mobile Endgeräte.....	251
14.1.1	Angriffe auf LTE- und 5G-Mobilfunknetze.....	252
14.1.2	Pegasus Spyware	252
14.2	Bekannte IoT-Hacks	253
14.2.1	Mirai Botnet (aka Dyn Attack).....	253
14.2.2	Kardiologische Überwachungsgeräte	254
14.2.3	Überwachungsgeräte der Herzfunktion von Babys	254
14.2.4	TRENDnet WebCam Hack	255
14.2.5	Jeep Hack	255
14.2.6	Verkada-Einbruch.....	255
14.2.7	Alexa vs. Alexa	256

14.3	Verschlüsselungsangriffe	256
14.3.1	WannaCry	256
14.3.2	Uni Maastricht	257
14.3.3	Ransomwareangriff auf ein Universitätsklinikum	259
14.3.4	DarkSide	259
14.4	Weitere bekannte Cyberangriffe	260
14.4.1	SolarWinds	260
14.4.2	DDoS-Angriff auf einen belgischen Internetprovider	262
14.4.3	Log4J	262
14.4.4	Fernüberwachung von Windkraftanlagen	263
14.4.5	DDoS-Schutzgelderpressung	264
	Literatur	265
A Open Source Werkzeuge		267
B Mounten von logischen Volumes für forensische Untersuchungen		279
C Zusammenstellung wichtiger Hyperlinks rund um die IT-Sicherheit		283
Stichwortverzeichnis		285