

Auf einen Blick

Einleitung	27
Teil I: Erste Schritte in Cybersicherheit	31
Kapitel 1: Was ist eigentlich Cybersicherheit?	33
Kapitel 2: Die häufigsten Cyberangriffe	47
Kapitel 3: Den Feind kennenlernen	69
Teil II: Ihre persönliche Sicherheit verbessern	87
Kapitel 4: Bewertung Ihrer aktuellen Sicherheitslage	89
Kapitel 5: Physische Sicherheit verbessern	109
Kapitel 6: Cybersicherheit im Homeoffice	119
Teil III: Schützen Sie sich – vor sich selbst	129
Kapitel 7: Ihre Konten sichern	131
Kapitel 8: Passwörter	147
Kapitel 9: Social Engineering verhindern	163
Kapitel 10: Cybersicherheit für Selbstständige und Freiberufler	181
Kapitel 11: Neue Technologien bringen neue Gefahren	189
Teil IV: Einen Sicherheitsvorfall händeln	199
Kapitel 12: Einen Sicherheitsvorfall erkennen	201
Kapitel 13: Nach einem Sicherheitsvorfall	219
Teil V: Backups und Wiederherstellung	235
Kapitel 14: Backups	237
Kapitel 15: Geräte zurücksetzen	263
Kapitel 16: Aus Backups wiederherstellen	273
Teil VI: Der Top-Ten-Teil	295
Kapitel 17: Zehn Tipps zur Verbesserung Ihrer Cybersicherheit	297
Kapitel 18: Zehn Erkenntnisse aus fünf Sicherheitsvorfällen	303
Kapitel 19: Zehn Tipps für die Nutzung eines öffentlichen WLANs	309

14 Auf einen Blick

Kapitel 20: Zehn Auswirkungen, die KI auf die Cybersicherheit
hat (und umgekehrt) 313

Abbildungsverzeichnis **325**

Stichwortverzeichnis **329**

Inhaltsverzeichnis

Einleitung	27
Über dieses Buch	27
Wie dieses Buch aufgebaut ist	28
Törichte Annahmen über die Leser	29
Konventionen in diesem Buch	29
Symbole, die in diesem Buch verwendet werden	29
Wie es weitergeht	30
TEIL I	
ERSTE SCHRITTE IN CYBERSICHERHEIT	31
Kapitel 1	
Was ist eigentlich Cybersicherheit?	33
Cybersicherheit definieren	33
Entwicklung von Cybersicherheit	35
Technologischer Wandel	35
Gesellschaftlicher Wandel	39
Wandel von Geschäftsmodellen	39
Politischer Wandel	40
Risiken mit Cybersicherheit minimieren	43
Die Ziele von Cybersicherheit: Die CIA-Triade	43
Risiken für den Menschen	44
Kapitel 2	
Die häufigsten Cyberangriffe	47
Angriffe, die Ihnen Schaden zufügen	47
Denial-of-Service-Angriffe (DoS)	48
Distributed-Denial-of-Service-Angriffe (DDoS)	48
Botnetze und Zombies	50
Datenzerstörungsangriffe	50
Angriffe auf physische Strukturen	51
Identitätsmissbrauch	51
Fake-Websites	51
Phishing	52
Spear-Phishing	52
CEO-Fraud	53
Smishing	54
Vishing	54
Tampering	54
Abfangen von Daten	54
Deep Fakes	55

16 Inhaltsverzeichnis

Datendiebstahl.....	56
Diebstahl persönlicher Daten.....	56
Diebstahl geschäftlicher Daten.....	57
Malware.....	57
Viren.....	58
Würmer.....	58
Trojaner.....	58
Ransomware.....	58
Scareware.....	59
Spyware.....	60
Kryptominer.....	60
Adware.....	60
Blended Malware.....	61
Zero-Day-Malware.....	61
Poisoned-Web-Service-Angriffe.....	61
Poisoning-Angriffe auf Netzwerkinfrastrukturen.....	62
Malvertising.....	62
Drive-by-Downloads.....	63
Diebstahl von Passwörtern.....	63
Mangelnde Wartung als Einfallstor – und gefälschte oder fehlerhafte Updates.....	65
Fortgeschrittene Angriffe.....	65
Opportunistische Angriffe.....	66
Gezielte Angriffe.....	66
Gemischte Angriffe (opportunistisch und gezielt).....	67

Kapitel 3 **Den Feind kennenlernen..... 69**

Von bösen und von guten Jungs.....	69
Eine kurze Bösewicht-Kunde.....	71
Script-Kiddies.....	71
Hacker, die keine Kiddies sind.....	71
Nationen und Staaten.....	72
Wirtschaftsspione.....	72
Kriminelle.....	72
Hacktivisten.....	73
Hacker und ihre bunten Hüte.....	74
Wie Hacker Geld verdienen.....	75
Direkter Finanzbetrug.....	75
Indirekter Finanzbetrug.....	76
Ransomware.....	78
Kryptominer.....	79
Umgang mit unabsichtlichen Bedrohungen.....	79
Menschliches Versagen.....	79
Externe Katastrophen.....	81
Angreifer abwehren.....	85
Risiken mit verschiedenen Methoden begegnen.....	86

**TEIL II
IHRE PERSÖNLICHE SICHERHEIT VERBESSERN 87**

**Kapitel 4
Bewertung Ihrer aktuellen Sicherheitslage 89**

- Die Bestandsaufnahme 89
 - Heimcomputer 90
 - Mobilgeräte 91
 - Gaming-Systeme 91
 - Geräte aus dem Universum des Internets der Dinge 91
 - Netzwerkausrüstung 92
 - Arbeitsumgebung 92
 - Social Engineering 92
- Risiken erkennen 92
- Gefahrenabwehr 93
 - Verteidigung des Perimeters 93
 - Router mit Firewall 93
 - Sicherheitssoftware 95
 - Richtige Konfiguration 95
 - Physischer Schutz Ihres Computers 96
 - Backups 97
 - Gefahr erkannt, Gefahr gebannt 97
 - Wiederherstellen 97
 - Aus Fehlern lernen 97
- Bewertung Ihrer aktuellen Sicherheitsmaßnahmen 98
 - Software 98
 - Hardware 99
 - Versicherung 100
 - Wissen ist Macht 100
- Privatsphäre 100
 - Erst nachdenken, dann teilen 101
 - Erst nachdenken, dann posten 101
 - Allgemeine Tipps zum Schutz der Privatsphäre 102
- Sicheres Onlinebanking 104
- Grundlagen der Sicherheit für Kryptowährungen 105
- Smart und sicher 106

**Kapitel 5
Physische Sicherheit verbessern 109**

- Die Bedeutung des physischen Schutzes verstehen 109
- Bestandsaufnahme 110
 - Ortsfeste Geräte 111
 - Mobile Geräte 112
- Gefährdete Daten identifizieren 112
- Einen Plan für physische Sicherheit erstellen 113
- Physische Sicherheit umsetzen 114
- Sicherheit für mobile Geräte 116
- Mitwisser sind die größte Gefahr 116

Kapitel 6	
Cybersicherheit im Homeoffice	119
Netzwerksicherheit im Homeoffice	119
Gerätesicherheit im Homeoffice	121
Physische Sicherheit im Homeoffice	122
Shoulder Surfing	122
Abhören (Eavesdropping)	123
Diebstahl	123
Menschliche Fehler	123
Sicherheit in Videokonferenzen	124
Private Dinge aus dem Kamerabild heraushalten	124
Videokonferenzen vor unbefugten Besuchern schützen	125
Stummschalten und Kamera blockieren	126
Aufzeichnungen	126
Social Engineering	126
Regulatorische Anforderungen	127

TEIL III

SCHÜTZEN SIE SICH – VOR SICH SELBST

129

Kapitel 7	
Ihre Konten sichern	131
Wiegen Sie sich nicht in falscher Sicherheit – Sie sind ein Ziel!	131
Externe Konten sichern	132
Daten in Nutzerkonten sichern	132
Seriöse Anbieter	133
Offizielle Apps und vertrauenswürdige Softwarequellen	133
Root und Jailbreak – keine gute Idee	133
Sparsam mit sensiblen Daten umgehen	134
Sichere Zahlungsdienstleister nutzen	134
Konten überwachen und Verdächtiges melden	134
Passwortstrategie und Zwei-Faktor-Authentifizierung	134
Abmelden, bitte!	136
Mein Computer, mein Telefon	137
Getrennte Computer und getrennte Browser	137
Geräte sichern	137
Software aktualisieren	137
Aufgepasst bei öffentlichen WLAN-Netzwerken	138
Sich selbst Grenzen setzen	139
Benachrichtigungen aktivieren	139
Wer war bei meinem Konto angemeldet?	139
Auf Betrugsalarm reagieren	140
Verschlüsselte Websites besuchen	140
Vor Social Engineering schützen	141
Links sind tabu	141
Social Media mit Sinn und Verstand	142
Datenschutzerklärungen lesen	142

Daten schützen bei Anbietern, mit denen Sie interagiert haben 143
 Daten schützen bei Anbietern, mit denen Sie nicht interagiert haben 144
 Vorsicht mit Hardware unbekannter Herkunft 146

**Kapitel 8
 Passwörter 147**

Passwörter – die ursprüngliche Authentifizierung 147
 Einfache Passwörter vermeiden 148
 Überlegungen zum Thema Passwörter 149
 Leicht zu erratende Passwörter 149
 Komplizierte Passwörter sind nicht immer besser 149
 Unterschiedliche Passwörter für unterschiedliche Zwecke 150
 Was ist ein sensibles Konto? 151
 Passwörter mehrfach verwenden – ab und zu erlaubt 151
 Mit Passwortmanagern das Gedächtnis entlasten 152
 Einprägsame und starke Passwörter 153
 Passwörter ändern – wann und wie oft 153
 Passwort nach einem Vorfall ändern 154
 Passwörter an Menschen weitergeben 155
 Passwörter speichern 155
 Passwörter übermitteln 156
 Alternativen für Passwörter finden 156
 Biometrische Authentifizierung 156
 SMS-basierte Authentifizierung 159
 App-basierte Einmalpasswörter 159
 Authentifizierung mit Hardware-Token 159
 USB-basierte Authentifizierung 160
 Passkeys von Google 160
 Auch Multifaktor-Authentifizierung hat Schwachstellen 161

**Kapitel 9
 Social Engineering verhindern 163**

Technologie ist nicht vertrauenswürdig 163
 Formen von Social-Engineering-Angriffen 164
 Die sechs Prinzipien des Social Engineerings 167
 Freigiebigkeit in den sozialen Medien 168
 Kalender und Reisepläne 169
 Finanzinformationen 169
 Persönliche Informationen 170
 Berufliche Informationen 171
 Medizinische oder juristische Ratschläge 171
 Standort 172
 Vorsicht bei viralen Trends 172
 Falsche Kontakte in den sozialen Netzwerken 172
 Foto 173
 Verifizierung 174
 Gemeinsame Freunde oder Kontakte 174
 Relevante Beiträge 174

Anzahl der Kontakte	174
Branche und Wohnort	175
Ähnliche Anfragen	175
Duplikate	175
Kontaktinformationen	176
LinkedIn-Premium-Status und -Empfehlungen	176
Gruppenaktivitäten	176
Stimmen die Verhältnisse?	176
Was macht einen Menschen zum Menschen?	177
Klischeehafte Namen	177
Kenntnisse	177
Rechtschreibung	178
Verdächtige Laufbahn	178
Prominente	178
Deep Fakes und virtuelles Kidnapping	179
Sicherheit durch falsche Informationen	179
Sicherheitssoftware	180
Allgemeine Cyberhygiene	180

Kapitel 10 Cybersicherheit für Selbstständige und Freiberufler 181

Cybersicherheit ist Ihre Verantwortung	181
Versicherung gegen Cyberschäden	181
Gesetze und Vorschriften einhalten	182
Datenschutzgrundverordnung und ePrivacy-Richtlinie	182
Bundesdatenschutzgesetz	183
Internetzugriff regeln	183
Gastzugang	184
Eingehende Verbindungen	184
Gegen DoS-Angriffe verteidigen	186
Website mit HTTPS	186
Fernzugriff auf Systeme	186
Vorsicht bei IoT-Geräten	186
Verschiedene Netzwerke	187
Vorsicht bei Kartenzahlung	187
Gegen Stromausfall sichern	187

Kapitel 11 Neue Technologien bringen neue Gefahren 189

Das Internet der Dinge	189
Kryptowährungen und Blockchain	191
Künstliche Intelligenz	193
Wachsender Bedarf für Cybersicherheit	194
Einsatz als Cybersicherheitstool	195
Einsatz als Hacking-Tool	195
Virtual Reality erleben	196
Augmented Reality erleben	197

**TEIL IV
EINEN SICHERHEITSVORFALL HÄNDELN 199**

**Kapitel 12
Einen Sicherheitsvorfall erkennen 201**

- Offensichtliche Vorfälle erkennen 201
 - Ransomware 202
 - Defacement 203
 - Angebliche Zerstörung von Daten 203
- Versteckte Vorfälle erkennen 204
 - Verlangsamtes Gerät 204
 - Kein Start des Task-Managers 205
 - Kein Start des Registrierungs-Editors 206
 - Probleme mit Latenz 206
 - Verbindungsprobleme und Buffering 207
 - Geänderte Geräteeinstellungen 208
 - Versand und Empfang seltsamer E-Mails 208
 - Versand und Empfang seltsamer Textnachrichten 208
 - Neue und unbekannte Software 208
 - Akkuprobleme und Hitzeentwicklung 209
 - Veränderte Dateien 209
 - Ungewöhnliche Darstellung von Websites 209
 - Unerwarteter Proxy-Server 210
 - Fehlerhafte Programme und Apps 210
 - Deaktivierte Sicherheitsprogramme 211
 - Erhöhter Datenverbrauch und Anzahl der SMS 211
 - Erhöhter Netzwerkverkehr 211
 - Ungewöhnliche geöffnete Ports 212
 - Häufige Systemabstürze 212
 - Ungewöhnlich hohe Telefonrechnung 213
 - Zugriffsanforderung durch unbekannte Programme 213
 - Aktivierung externer Geräte 213
 - Wer hat die Kontrolle über Ihr Gerät? 213
 - Neue Standardsuchmaschine 213
 - Geändertes Gerätepasswort 214
 - Aufdringliche Popups 214
 - Neue Browser-Add-on 215
 - Neue Browser-Startseite 215
 - Blockierung von E-Mails durch Spamfilter 215
 - Zugriff auf problematische Websites 216
 - Ungewöhnliche Unterbrechungen 216
 - Geänderte Spracheinstellungen 217
 - Unerklärliche Geräteaktivitäten 217
 - Unerklärliche Online-Aktivitäten 217
 - Plötzliche Neustarts 217
 - Bekanntes Datenleck 217

22 Inhaltsverzeichnis

Weiterleitung zur falschen Website	217
Ein brennendes Festplattenlämpchen	218
Anderes abnormales Verhalten	218

Kapitel 13 **Nach einem Sicherheitsvorfall 219**

Vorsicht ist besser als Nachsicht	219
Ruhig und besonnen handeln	219
Einen Profi engagieren	220
Maßnahmen ohne professionelle Unterstützung	220
Schritt 1: Was ist passiert (oder passiert gerade)?	221
Schritt 2: Den Angriff eindämmen	221
Schritt 3: Den Angriff beenden und beseitigen	223
Beschädigte Software neu installieren	226
Neustart und Scan	226
Problematische Wiederherstellungspunkte löschen	227
Einstellungen wiederherstellen	227
System neu aufsetzen	228
Umgang mit gestohlenen Daten	228
Lösegeld zahlen – oder nicht?	230
Lehren für die Zukunft	230
Umgang mit Datenlecks eines Anbieters	230
Grund für die Mitteilung	231
Vorfälle rufen Betrüger auf den Plan	231
Passwörter	232
Zahlungsdaten	232
Dokumente von Behörden	233
Dokumente von Uni oder Arbeitgeber	233
Konten in den sozialen Medien	233

TEIL V **BACKUPS UND WIEDERHERSTELLUNG 235**

Kapitel 14 **Backups 237**

Backups sind Pflicht und keine Kür	237
Backups von Daten aus Apps und Online-Konten	238
SMS-Nachrichten	238
Soziale Medien	239
WhatsApp	239
Google Photos	240
Andere Apps	240
Backups in die und aus der Cloud	240
Sicherung von Daten in Cloud-Konten	240
Sicherung von Daten aus Cloud-Konten	241
Backups von Smartphones	241

Backups von Kryptowährungen	242
Sicherung von Passwörtern	242
Verschiedene Formen von Backups	243
Vollständige Systemsicherung	243
Wiederherstellungsimage	244
Später erstellte Systemimages	244
Original-Installationsmedien	244
Heruntergeladene Software	245
Vollständiges Daten-Backup	245
Inkrementelles Backup	246
Differenzielles Backup	246
Gemischte Backups	246
Kontinuierliche Backups	247
Partielle Backups	247
Backups von Ordnern	248
Backups von Laufwerken	248
Backups von virtuellen Laufwerken	249
Ausnahmen	250
Programminterne Backup-Funktionen	250
Backup-Tools kennenlernen	251
Backup-Software	251
Laufwerksspezifische Backup-Software	252
Windows-Sicherung	252
Smartphone- und Tablet-Backup	253
Manuelles Kopieren von Dateien oder Ordnern	253
Automatisiertes Kopieren von Dateien oder Ordnern	254
Backups von Drittanbietern	254
Der richtige Aufbewahrungsort für Backups	254
Lokale Aufbewahrung	255
Offsite-Aufbewahrung	255
Cloud-Backups	256
Netzwerkspeicherung	256
Verschiedene Aufbewahrungsorte	257
Tabus für die Aufbewahrung von Backups	257
Verschlüsselung von Backups	258
Häufigkeit von Backups	258
Backups entsorgen	259
Backups testen	261
Ein Bootmedium erstellen	261

Kapitel 15	
Geräte zurücksetzen	263
Die zwei Arten des Zurücksetzens	263
Soft Reset	264
Hard Reset	266
Ein Gerät nach einem Hard Reset neu einrichten	272

Kapitel 16	
Aus Backups wiederherstellen	273
Der Tag der Wiederherstellung wird kommen	273
Warten Sie mit der Wiederherstellung!	274
Inventarisierung Ihrer Backups	274
Eine vollständige Systemsicherung wiederherstellen	275
Wiederherstellung auf dem gleichen Gerät	275
Wiederherstellung auf einem anderen Gerät	275
Wiederherstellungsimagen	276
Wiederherstellung aus später erstellten Systemimages	277
Sicherheitssoftware installieren	277
Original-Installationsmedien	277
Heruntergeladene Software	278
Wiederherstellung aus einem vollständigen Daten-Backup	278
Wiederherstellung aus inkrementellen Backups	279
Inkrementelle Backups von Daten	280
Inkrementelle Backups von Systemen	280
Wiederherstellung aus differenziellen Backups	280
Wiederherstellung aus kontinuierlichen Backups	281
Wiederherstellung aus partiellen Backups	282
Wiederherstellung aus Ordner-Backups	282
Wiederherstellung von Laufwerk-Backups	283
Wiederherstellung aus virtuellen Laufwerken	283
Umgang mit gelöschten Dateien	284
Ausschluss von Dateien und Ordnern	285
Wiederherstellung aus programminternen Backups	286
Archive verstehen	286
Viele Dateien in einer Datei	286
Alte Daten	287
Alte Datei-, Ordner- oder Backup-Versionen	287
Wiederherstellung mit Backup-Tools	287
Wiederherstellung aus dem Dateiversionsverlauf	288
Rückkehr zu einem Wiederherstellungspunkt	288
Wiederherstellung aus einem Smartphone-/Tablet-Backup	289
Wiederherstellung aus einem manuellen Datei- oder Ordner-Backup	290
Wiederherstellung von Backups bei Cloudanbietern	290
Backups an ihren Ort zurückbringen	290
Netzwerksspeicherung	291
Wiederherstellung aus verschiedenen Backups	291
Wiederherstellung auf anderem Gerät testen	291
Wiederherstellung aus verschlüsselten Backups	291
Wiederherstellung von Kryptowährungen	292
Booten von einem Bootmedium	293
Nach der Wiederherstellung	293

TEIL VI DER TOP-TEN-TEIL..... 295

Kapitel 17 Zehn Tipps zur Verbesserung Ihrer Cybersicherheit..... 297

Sie sind ein Ziel!	297
Sicherheitssoftware benutzen	297
Sensible Daten verschlüsseln	298
Backups, Backups, Backups	299
Eigene Anmeldedaten	300
Auf sichere Authentifizierung achten	300
Vorsicht im Umgang mit sozialen Netzwerken	301
Netzwerk aufteilen	301
Öffentliches WLAN sicher nutzen (oder besser gar nicht)	301
Einen Experten engagieren	301

Kapitel 18 Zehn Erkenntnisse aus fünf Sicherheitsvorfällen..... 303

Die Hotelkette Marriott	303
Der Einzelhändler Target	304
Die Filmstudios Sony Pictures	305
Die Regierungsbehörde OPM	306
Die Krankenversicherung Anthem	307

Kapitel 19 Zehn Tipps für die Nutzung eines öffentlichen WLANs..... 309

Das Handy als mobilen Hotspot nutzen	310
WLAN-Verbindung bei Nichtbenutzung deaktivieren	310
Keine sensiblen Aufgaben	310
Einen VPN-Dienst nutzen	311
Einen Reise-Router nutzen	311
Tor-Browser verwenden	311
Verschlüsseln	311
Netzwerkfreigaben deaktivieren	311
Sicherheitssoftware installieren	312
Öffentlich ist nicht gleich öffentlich	312

Kapitel 20 Zehn Auswirkungen, die KI auf die Cybersicherheit hat (und umgekehrt)..... 313

KI verändert das Spielfeld der Cybersicherheit grundlegend	315
KI stärkt die Verteidigung	316
KI wird zugleich zum Werkzeug für Angreifer	317
KI macht Social Engineering realistischer und »persönlicher«	318
KI automatisiert und verfeinert technische Angriffe	318
KI entwickelt Exploits fast in Echtzeit	319

26 Inhaltsverzeichnis

KI erzeugt neue physische Sicherheitsrisiken	320
KI erhöht den Bedarf an starker Cybersicherheit.	321
KI stellt die Grundlagen menschlicher Kreativität infrage	321
KI hat weitere Folgen, die wir noch nicht absehen können.	322
Abbildungsverzeichnis	325
Stichwortverzeichnis	329