

# Auf einen Blick

---

<b>Über den Autor</b> .....	<b>9</b>
<b>Einleitung</b> .....	<b>23</b>
<b>Teil I: Erste Schritte in Cybersicherheit</b> .....	<b>27</b>
<b>Kapitel 1:</b> Was ist eigentlich Cybersicherheit? .....	29
<b>Kapitel 2:</b> Die häufigsten Cyberangriffe .....	41
<b>Kapitel 3:</b> Den Feind kennenlernen .....	61
<b>Teil II: Ihre persönliche Sicherheit verbessern</b> .....	<b>79</b>
<b>Kapitel 4:</b> Bewertung Ihrer aktuellen Sicherheitslage .....	81
<b>Kapitel 5:</b> Physische Sicherheit verbessern .....	99
<b>Teil III: Schützen Sie sich – vor sich selbst</b> .....	<b>109</b>
<b>Kapitel 6:</b> Ihre Konten sichern .....	111
<b>Kapitel 7:</b> Passwörter .....	127
<b>Kapitel 8:</b> Social Engineering verhindern .....	141
<b>Kapitel 9:</b> Cybersicherheit für Selbstständige und Freiberufler .....	159
<b>Kapitel 10:</b> Neue Technologien bringen neue Gefahren .....	167
<b>Teil IV: Einen Sicherheitsvorfall händeln</b> .....	<b>177</b>
<b>Kapitel 11:</b> Einen Sicherheitsvorfall erkennen .....	179
<b>Kapitel 12:</b> Nach einem Sicherheitsvorfall .....	197
<b>Teil V: Backups und Wiederherstellung</b> .....	<b>213</b>
<b>Kapitel 13:</b> Backups .....	215
<b>Kapitel 14:</b> Geräte zurücksetzen .....	237
<b>Kapitel 15:</b> Aus Backups wiederherstellen .....	247
<b>Teil VI: Der Top-Ten-Teil</b> .....	<b>267</b>
<b>Kapitel 16:</b> Zehn Tipps zur Verbesserung Ihrer Cybersicherheit .....	269
<b>Kapitel 17:</b> Zehn Erkenntnisse aus fünf Sicherheitsvorfällen .....	275
<b>Kapitel 18:</b> Zehn Tipps für die Nutzung eines öffentlichen WLANs .....	281
<b>Stichwortverzeichnis</b> .....	<b>285</b>



# Inhaltsverzeichnis

---

<b>Über den Autor</b> .....	<b>9</b>
<b>Einleitung</b> .....	<b>23</b>
Über dieses Buch .....	23
Wie dieses Buch aufgebaut ist .....	24
Törichte Annahmen über den Leser .....	24
Konventionen in diesem Buch .....	25
Symbole, die in diesem Buch verwendet werden .....	25
Wie es weitergeht .....	25
<b>TEIL I</b>	
<b>ERSTE SCHRITTE IN CYBERSICHERHEIT</b> .....	<b>27</b>
<b>Kapitel 1</b>	
<b>Was ist eigentlich Cybersicherheit?</b> .....	<b>29</b>
Cybersicherheit definieren .....	29
Entwicklung von Cybersicherheit .....	30
Technologischer Wandel .....	31
Gesellschaftlicher Wandel .....	33
Wandel von Geschäftsmodellen .....	34
Politischer Wandel .....	34
Risiken mit Cybersicherheit minimieren .....	38
Die Ziele von Cybersicherheit: Die CIA-Triade .....	38
Risiken für den Menschen .....	39
<b>Kapitel 2</b>	
<b>Die häufigsten Cyberangriffe</b> .....	<b>41</b>
Angriffe, die Ihnen Schaden zufügen .....	41
Denial-of-Service-Angriffe (DoS) .....	42
Distributed-Denial-of-Service-Angriffe (DDoS) .....	42
Botnetze und Zombies .....	44
Datenzerstörungsangriffe .....	44
Identitätsmissbrauch .....	45
Fake-Websites .....	45
Phishing .....	46
Spear-Phishing .....	46
CEO-Fraud .....	46
Smishing .....	47
Vishing .....	47
Tampering .....	47
Abfangen von Daten .....	48

## 14 Inhaltsverzeichnis

Datendiebstahl.....	49
Diebstahl persönlicher Daten.....	49
Diebstahl geschäftlicher Daten.....	49
Malware.....	51
Viren.....	51
Würmer.....	51
Trojaner.....	51
Ransomware.....	52
Scareware.....	53
Spyware.....	53
Kryptominer.....	53
Adware.....	54
Blended Malware.....	54
Zero-Day-Malware.....	54
Poisoned-Web-Service-Angriffe.....	54
Poisoning-Angriffe auf Netzwerkinfrastrukturen.....	55
Malvertising.....	56
Drive-by-Downloads.....	56
Diebstahl von Passwörtern.....	57
Mangelnde Wartung als Einfallstor.....	58
Fortgeschrittene Angriffe.....	58
Opportunistische Angriffe.....	59
Gezielte Angriffe.....	59
Gemischte Angriffe (opportunistisch und gezielt).....	60

## Kapitel 3

<b>Den Feind kennenlernen.....</b>	<b>61</b>
Von bösen und von guten Jungs.....	61
Böse Jungs, die nichts Gutes im Schilde führen.....	63
Script-Kiddies.....	63
Hacker, die keine Kiddies sind.....	63
Nationen und Staaten.....	64
Wirtschaftsspione.....	64
Kriminelle.....	64
Hacktivisten.....	65
Hacker und ihre bunten Hüte.....	66
Wie Hacker Geld verdienen.....	67
Direkter Finanzbetrug.....	67
Indirekter Finanzbetrug.....	68
Ransomware.....	70
Kryptominer.....	71
Umgang mit nicht-bösartigen Bedrohungen.....	71
Menschliches Versagen.....	71
Externe Katastrophen.....	73
Angreifer abwehren.....	77
Risiken mit verschiedenen Methoden begegnen.....	78

**TEIL II  
IHRE PERSÖNLICHE SICHERHEIT VERBESSERTEN..... 79**

**Kapitel 4  
Bewertung Ihrer aktuellen Sicherheitslage..... 81**

- Die Bestandsaufnahme ..... 81
  - Heimcomputer ..... 82
  - Mobilgeräte..... 82
  - Gaming-Systeme ..... 83
  - Geräte aus dem Universum des Internets der Dinge..... 83
  - Netzwerkausrüstung ..... 83
  - Arbeitsumgebung..... 84
  - Social Engineering ..... 84
- Risiken erkennen ..... 84
- Gefahrenabwehr ..... 84
  - Verteidigung des Perimeters ..... 85
  - Router mit Firewall..... 85
  - Sicherheitssoftware ..... 87
  - Physischer Schutz Ihres Computers ..... 87
  - Backups..... 88
  - Gefahr erkannt, Gefahr gebannt ..... 88
  - Wiederherstellen ..... 88
  - Aus Fehlern lernen..... 88
- Bewertung Ihrer aktuellen Sicherheitsmaßnahmen ..... 88
  - Software ..... 89
  - Hardware..... 90
  - Versicherung..... 90
  - Wissen ist Macht..... 91
- Privatsphäre..... 91
  - Erst nachdenken, dann teilen..... 91
  - Erst nachdenken, dann posten ..... 92
  - Allgemeine Tipps zum Schutz der Privatsphäre ..... 93
- Sicheres Onlinebanking ..... 95
- Smart und sicher ..... 96

**Kapitel 5  
Physische Sicherheit verbessern..... 99**

- Die Bedeutung des physischen Schutzes verstehen ..... 99
- Bestandsaufnahme ..... 100
  - Ortsfeste Geräte..... 101
  - Mobile Geräte..... 101
- Gefährdete Daten identifizieren ..... 102
- Einen Plan für physische Sicherheit erstellen ..... 103
- Physische Sicherheit umsetzen ..... 104
- Sicherheit für mobile Geräte ..... 106
- Mitwisser sind die größte Gefahr ..... 106

## TEIL III SCHÜTZEN SIE SICH – VOR SICH SELBST ..... 109

### Kapitel 6 Ihre Konten sichern ..... 111

Wiegen Sie sich nicht in falscher Sicherheit – Sie sind ein Ziel! .....	111
Externe Konten sichern .....	112
Daten in Nutzerkonten sichern .....	112
Seriose Anbieter .....	113
Offizielle Apps und vertrauenswürdige Softwarequellen .....	113
Root und Jailbreak – keine gute Idee .....	113
Sparsam mit sensiblen Daten umgehen .....	113
Sichere Zahlungsdienstleister nutzen .....	114
Konten überwachen und Verdächtiges melden .....	114
Passwortstrategie und Zwei-Faktor-Authentifizierung .....	114
Abmelden, bitte! .....	116
Mein Computer, mein Telefon .....	117
Getrennte Computer und getrennte Browser .....	117
Geräte sichern .....	117
Software aktualisieren .....	117
Aufgepasst bei öffentlichen WLAN-Netzwerken .....	118
Sich selbst Grenzen setzen .....	119
Benachrichtigungen aktivieren .....	119
Wer war bei meinem Konto angemeldet? .....	119
Auf Betrugsalarm reagieren .....	120
Verschlüsselte Websites besuchen .....	120
Vor Social Engineering schützen .....	121
Links sind tabu .....	121
Social Media mit Sinn und Verstand .....	122
Datenschutzerklärungen lesen .....	122
Daten schützen bei Anbietern, mit denen Sie interagiert haben .....	123
Daten schützen bei Anbietern, mit denen Sie nicht interagiert haben .....	124

### Kapitel 7 Passwörter ..... 127

Passwörter – die ursprüngliche Authentifizierung .....	127
Einfache Passwörter vermeiden .....	128
Überlegungen zum Thema Passwörter .....	128
Leicht zu erratende Passwörter .....	129
Komplizierte Passwörter sind nicht immer besser .....	130
Unterschiedliche Passwörter für unterschiedliche Zwecke .....	130
Was ist ein sensibles Konto? .....	131
Passwörter mehrfach verwenden – ab und zu erlaubt .....	131
Mit Passwortmanagern das Gedächtnis entlasten .....	131
Einprägsame und starke Passwörter .....	132
Passwörter ändern – wann und wie oft .....	133
Passwort nach einem Vorfall ändern .....	134
Passwörter an Menschen weitergeben .....	135
Passwörter speichern .....	135

Passwörter übermitteln . . . . .	135
Alternativen für Passwörter finden . . . . .	136
Biometrische Authentifizierung . . . . .	136
SMS-basierte Authentifizierung . . . . .	138
App-basierte Einmalpasswörter . . . . .	138
Authentifizierung mit Hardware-Token . . . . .	138
USB-basierte Authentifizierung . . . . .	139

**Kapitel 8  
Social Engineering verhindern . . . . . 141**

Technologie ist nicht vertrauenswürdig . . . . .	141
Formen von Social-Engineering-Angriffen . . . . .	141
Die sechs Prinzipien des Social Engineerings . . . . .	145
Freigiebigkeit in den sozialen Medien . . . . .	146
Kalender und Reisepläne . . . . .	146
Finanzinformationen . . . . .	147
Persönliche Informationen . . . . .	147
Berufliche Informationen . . . . .	149
Medizinische oder juristische Ratschläge . . . . .	149
Standort . . . . .	149
Vorsicht bei viralen Trends . . . . .	150
Falsche Kontakte in den sozialen Netzwerken . . . . .	150
Foto . . . . .	151
Verifizierung . . . . .	151
Gemeinsame Freunde oder Kontakte . . . . .	151
Relevante Beiträge . . . . .	152
Anzahl der Kontakte . . . . .	152
Branche und Wohnort . . . . .	152
Ähnliche Anfragen . . . . .	153
Duplikate . . . . .	153
Kontaktinformationen . . . . .	153
LinkedIn-Premium-Status und -Empfehlungen . . . . .	153
Gruppenaktivitäten . . . . .	154
Stimmen die Verhältnisse? . . . . .	154
Was macht einen Menschen zum Menschen? . . . . .	154
Klischeehafte Namen . . . . .	155
Kenntnisse . . . . .	155
Rechtschreibung . . . . .	155
Verdächtige Laufbahn . . . . .	155
Prominente . . . . .	156
Sicherheit durch falsche Informationen . . . . .	156
Sicherheitssoftware . . . . .	157
Allgemeine Cyberhygiene . . . . .	157

**Kapitel 9  
Cybersicherheit für Selbstständige und Freiberufler . . . . . 159**

Cybersicherheit ist Ihre Verantwortung . . . . .	159
Versicherung gegen Cyberschäden . . . . .	159

## 18 Inhaltsverzeichnis

Gesetze und Vorschriften einhalten .....	160
Datenschutzgrundverordnung .....	160
Bundesdatenschutzgesetz .....	161
Internetzugriff regeln .....	161
Gastzugang .....	161
Eingehende Verbindungen .....	162
Gegen DoS-Angriffe verteidigen .....	164
Website mit HTTPS .....	164
Fernzugriff auf Systeme .....	164
Vorsicht bei IoT-Geräten .....	164
Verschiedene Netzwerke .....	165
Vorsicht bei Kartenzahlung .....	165
Gegen Stromausfall sichern .....	165

### Kapitel 10

#### **Neue Technologien bringen neue Gefahren .....** 167

Das Internet der Dinge .....	167
Kryptowährungen und Blockchain .....	169
Künstliche Intelligenz .....	171
Wachsender Bedarf für Cybersicherheit .....	172
Einsatz als Cybersicherheitstool .....	173
Einsatz als Hacking-Tool .....	173
Virtual Reality erleben .....	174
Augmented Reality erleben .....	175

### TEIL IV

#### **EINEN SICHERHEITSVORFALL HÄNDELN .....** 177

### Kapitel 11

#### **Einen Sicherheitsvorfall erkennen .....** 179

Offensichtliche Vorfälle erkennen .....	179
Ransomware .....	180
Defacement .....	180
Angebliche Zerstörung von Daten .....	181
Versteckte Vorfälle erkennen .....	182
Verlangsamtes Gerät .....	182
Kein Start des Task-Managers .....	183
Kein Start des Registrierungs-Editors .....	183
Probleme mit Latenz .....	184
Verbindungsprobleme und Buffering .....	184
Geänderte Geräteeinstellungen .....	185
Versand und Empfang seltsamer E-Mails .....	186
Versand und Empfang seltsamer Textnachrichten .....	186
Neue und unbekannte Software .....	186
Akkuprobleme und Hitzeentwicklung .....	186
Veränderte Dateien .....	187
Ungewöhnliche Darstellung von Websites .....	187
Unerwarteter Proxy-Server .....	187



Fehlerhafte Programme und Apps .....	188
Deaktivierte Sicherheitsprogramme .....	188
Erhöhter Datenverbrauch und Anzahl der SMS .....	188
Erhöhter Netzwerkverkehr .....	189
Ungewöhnliche geöffnete Ports .....	189
Häufige Systemabstürze .....	190
Ungewöhnlich hohe Telefonrechnung .....	190
Zugriffsanforderung durch unbekannte Programme .....	190
Aktivierung externer Geräte .....	191
Wer hat die Kontrolle über Ihr Gerät? .....	191
Neue Standardsuchmaschine .....	191
Geändertes Gerätepasswort .....	191
Aufdringliche Popups .....	191
Neue Browser-Add-Ons .....	193
Neue Browser-Startseite .....	193
Blockierung von E-Mails durch Spamfilter .....	193
Zugriff auf problematische Websites .....	194
Ungewöhnliche Unterbrechungen .....	194
Geänderte Spracheinstellungen .....	194
Unerklärliche Geräteaktivitäten .....	194
Unerklärliche Online-Aktivitäten .....	194
Plötzliche Neustarts .....	195
Bekanntes Datenleck .....	195
Weiterleitung zur falschen Website .....	195
Ein brennendes Festplattenlämpchen .....	195
Anderes abnormales Verhalten .....	195

**Kapitel 12**  
**Nach einem Sicherheitsvorfall ..... 197**

Vorsicht ist besser als Nachsicht .....	197
Ruhig und besonnen handeln .....	197
Einen Profi engagieren .....	198
Maßnahmen ohne professionelle Unterstützung .....	198
Schritt 1: Was ist passiert (oder passiert gerade)? .....	199
Schritt 2: Den Angriff eindämmen .....	199
Schritt 3: Den Angriff beenden und beseitigen .....	201
Beschädigte Software neu installieren .....	204
Neustart und Scan .....	204
Problematische Wiederherstellungspunkte löschen .....	205
Einstellungen wiederherstellen .....	205
System neu aufsetzen .....	206
Umgang mit gestohlenen Daten .....	206
Lösegeld zahlen – oder nicht? .....	208
Lehren für die Zukunft .....	208
Umgang mit Datenlecks eines Anbieters .....	208
Grund für die Mitteilung .....	209
Vorfälle rufen Betrüger auf den Plan .....	209
Passwörter .....	210

Zahlungsdaten . . . . .	210
Dokumente von Behörden . . . . .	211
Dokumente von Uni oder Arbeitgeber . . . . .	211
Konten in den sozialen Medien . . . . .	211

## TEIL V BACKUPS UND WIEDERHERSTELLUNG . . . . . 213

### Kapitel 13 Backups . . . . . 215

Backups sind Pflicht und keine Kür . . . . .	215
Verschiedene Formen von Backups . . . . .	216
Vollständige Systemsicherung . . . . .	216
Wiederherstellungsimagen . . . . .	217
Später erstellte Systemimages . . . . .	217
Original-Installationsmedien . . . . .	217
Heruntergeladene Software . . . . .	218
Vollständiges Daten-Backup . . . . .	218
Inkrementelles Backup . . . . .	219
Differenzielles Backup . . . . .	219
Gemischte Backups . . . . .	220
Kontinuierliche Backups . . . . .	220
Partielle Backups . . . . .	220
Backups von Ordnern . . . . .	221
Backups von Laufwerken . . . . .	222
Backups von virtuellen Laufwerken . . . . .	222
Ausnahmen . . . . .	223
Programminterne Backup-Funktionen . . . . .	224
Backup-Tools kennenlernen . . . . .	224
Backup-Software . . . . .	224
Laufwerksspezifische Backup-Software . . . . .	225
Windows-Sicherung . . . . .	225
Smartphone- und Tablet-Backup . . . . .	226
Manuelles Kopieren von Dateien oder Ordnern . . . . .	226
Automatisiertes Kopieren von Dateien oder Ordnern . . . . .	227
Backups von Drittanbietern . . . . .	227
Der richtige Aufbewahrungsort für Backups . . . . .	228
Lokale Aufbewahrung . . . . .	228
Offsite-Aufbewahrung . . . . .	228
Cloud-Backups . . . . .	229
Netzwerksspeicherung . . . . .	229
Verschiedene Aufbewahrungsorte . . . . .	230
Tabus für die Aufbewahrung von Backups . . . . .	230
Verschlüsselung von Backups . . . . .	231
Häufigkeit von Backups . . . . .	232
Backups entsorgen . . . . .	232
Backups testen . . . . .	234
Backups von Kryptowährungen . . . . .	234

Backups von Passwörtern ..... 235  
 Ein Bootmedium erstellen ..... 235

**Kapitel 14**  
**Geräte zurücksetzen ..... 237**

Die zwei Arten des Zurücksetzens ..... 237  
     Soft Reset ..... 238  
     Hard Reset ..... 240  
 Ein Gerät nach einem Hard Reset neu einrichten ..... 245

**Kapitel 15**  
**Aus Backups wiederherstellen ..... 247**

Der Tag der Wiederherstellung wird kommen ..... 247  
 Warten Sie mit der Wiederherstellung! ..... 248  
 Eine vollständige Systemsicherung wiederherstellen ..... 248  
     Wiederherstellung auf dem gleichen Gerät ..... 249  
     Wiederherstellung auf einem anderen Gerät ..... 249  
     Wiederherstellungsimages ..... 250  
     Wiederherstellung aus später erstellen Systemimages ..... 250  
     Sicherheitssoftware installieren ..... 251  
     Original-Installationsmedien ..... 251  
     Heruntergeladene Software ..... 251  
     Wiederherstellung aus einem vollständigen Daten-Backup ..... 252  
 Wiederherstellung aus inkrementellen Backups ..... 253  
     Inkrementelle Backups von Daten ..... 253  
     Inkrementelle Backups von Systemen ..... 254  
     Wiederherstellung aus differenziellen Backups ..... 254  
     Wiederherstellung aus kontinuierlichen Backups ..... 255  
     Wiederherstellung aus partiellen Backups ..... 255  
     Wiederherstellung aus Ordner-Backups ..... 256  
     Wiederherstellung von Laufwerk-Backups ..... 256  
     Wiederherstellung aus virtuellen Laufwerken ..... 257  
 Umgang mit gelöschten Dateien ..... 258  
 Ausschluss von Dateien und Ordnern ..... 258  
 Wiederherstellung aus programminternen Backups ..... 259  
 Archive verstehen ..... 259  
     Viele Dateien in einer Datei ..... 260  
     Alte Daten ..... 260  
     Alte Datei-, Ordner- oder Backup-Versionen ..... 260  
 Wiederherstellung mit Backup-Tools ..... 261  
     Wiederherstellung aus dem Dateiversionsverlauf ..... 262  
     Rückkehr zu einem Wiederherstellungspunkt ..... 262  
     Wiederherstellung aus einem Smartphone-/Tablet-Backup ..... 262  
     Wiederherstellung aus einem manuellen Datei- oder Ordner-Backup ..... 263  
     Wiederherstellung von Backups bei Cloudanbietern ..... 264  
 Backups an ihren Ort zurückbringen ..... 264  
     Netzwerkspeicherung ..... 264  
     Wiederherstellung aus verschiedenen Backups ..... 265

## 22 Inhaltsverzeichnis

Wiederherstellung auf anderem Gerät testen .....	265
Wiederherstellung aus verschlüsselten Backups .....	265
Wiederherstellung von Kryptowährungen.....	265
Booten von einem Bootmedium.....	266

## TEIL VI DER TOP-TEN-TEIL..... 267

### Kapitel 16 Zehn Tipps zur Verbesserung Ihrer Cybersicherheit..... 269

Sie sind ein Ziel! .....	269
Sicherheitssoftware benutzen.....	270
Sensible Daten verschlüsseln .....	270
Backups, Backups, Backups .....	271
Eigene Anmeldedaten.....	272
Auf sichere Authentifizierung achten.....	272
Vorsicht im Umgang mit sozialen Netzwerken .....	272
Netzwerk aufteilen .....	273
Öffentliches WLAN sicher nutzen .....	273
Einen Experten engagieren .....	273

### Kapitel 17 Zehn Erkenntnisse aus fünf Sicherheitsvorfällen..... 275

Die Hotelkette Marriott.....	275
Der Einzelhändler Target .....	276
Die Filmstudios Sony Pictures .....	277
Die Regierungsbehörde OPM .....	278
Die Krankenversicherung Anthem .....	279

### Kapitel 18 Zehn Tipps für die Nutzung eines öffentlichen WLANs ..... 281 |

Das Handy als mobilen Hotspot nutzen.....	281
WLAN-Verbindung bei Nichtbenutzung deaktivieren .....	281
Keine sensiblen Aufgaben .....	282
Keine Passwörter zurücksetzen.....	282
Einen VPN-Dienst nutzen .....	282
Tor-Browser verwenden.....	282
Verschlüsseln .....	282
Netzwerkfreigaben deaktivieren.....	282
Sicherheitssoftware installieren .....	283
Öffentlich ist nicht gleich öffentlich .....	283

### Stichwortverzeichnis..... 285