



Auf einen Blick

Einleitung	21
Teil I: Grundlagen der Cybersicherheit	23
Kapitel 1: Zurück in die Zukunft? Bedrohungen im Wandel der Zeit.....	25
Kapitel 2: Alles, was Sie über Passwörter wissen müssen.....	35
Kapitel 3: My home is my castle: Das Heimnetzwerk sicher einrichten.....	55
Kapitel 4: Das Tor zum Internet: Browser, aber sicher.....	75
Kapitel 5: Sichere Bankgeschäfte im Internet.....	91
Kapitel 6: Kein Backup — kein Mitleid. So sichern Sie Ihre Daten richtig.....	99
Kapitel 7: Ihre Informationen in fremden Händen — Datenlecks.....	119
Kapitel 8: Endlich Endgeräte absichern und schützen.....	139
Teil II: Der Mensch im Fokus	157
Kapitel 9: Menschliche Sicherheit.....	159
Kapitel 10: Phishing-Mails — so erkennen Sie die falsche Nachricht.....	177
Kapitel 11: Vishing, Smishing, Chishing — die Familie Phishing wird größer.....	191
Kapitel 12: Ransomware — wenn der Rechner nur noch kryptisch spricht.....	197
Teil III: Lug und Betrug im Internet	209
Kapitel 13: Die Evergreens: Diese Betrugsmaschen gibt es schon ewig.....	211
Kapitel 14: One-Hit-Wonder: Auf diese Maschen fallen Sie garantiert nur einmal herein.....	219
Kapitel 15: Die Newcomer: Neue Technologien schaffen neue Betrugsmaschen.....	227
Kapitel 16: So bereiten Sie sich auf eine Ausnahmesituation vor.....	241
Teil IV: Der Top-Ten-Teil	245
Kapitel 17: Die 10 Tipps für ein sicheres Internet zu Hause.....	247
Kapitel 18: Die Top 10 Betrugsmaschen.....	255
Kapitel 19: Die Top 10 Tipps im Internet.....	263
Kapitel 20: Die Top 10 prominenten Datenlecks und was Sie daraus lernen können.....	267
Abbildungsverzeichnis	279
Stichwortverzeichnis	285







Inhaltsverzeichnis

Einleitung	21
Konventionen in diesem Buch	21
Symbole, die in diesem Buch verwendet werden	21
TEIL I	
GRUNDLAGEN DER CYBERSICHERHEIT	23
Kapitel 1	
Zurück in die Zukunft? Bedrohungen im Wandel der Zeit	25
Das ARPANET	26
Creepers – die erste Malware	27
Creepers	27
Reapers	27
Eine kurze Geschichte der Schadsoftware	28
Schadsoftware heutzutage	28
Wann man sicher ist	29
Risikomanagement	31
Der Prozess der Risikoerkennung	33
Kapitel 2	
Alles, was Sie über Passwörter wissen müssen	35
Passwörter – easy to learn, hard to master	36
Sicherheitsfragen sind kein Sicherheitsnetz	37
Mehrfachverwendung von Passwörtern	37
Methoden zur Erstellung von Passwörtern	38
Passwort-Manager – ein guter Kompromiss	42
Wann soll ich und wann muss ich das Passwort wechseln?	46
Die Zwei-Faktor-Authentifizierung – der zusätzliche Schutz	47
Diese Methoden eignen sich gut als zweiter Faktor	47
Passkeys — die modernisierten Passwörter?	51
Künstliche Intelligenz – eine Bedrohung für das Passwort	52
Kapitel 3	
My home is my castle: Das Heimnetzwerk sicher einrichten	55
Der Router – die Achillesferse des Heimnetzes	57
Freie Routerwahl in Deutschland	57
Aktualisierungen durchführen	57
Login-Portal finden und einloggen	58
Zugangspasswort zum Router ändern	62
Kabellose Netzwerke richtig absichern	63
Implementierung von WPA3 oder WPA2 im drahtlosen Netzwerk	64





12 Inhaltsverzeichnis

Einrichten und Verwenden von Gastnetzwerken.....	65
Ein (W)LAN für unterschiedliche Geräte.....	65
Deaktivieren Sie die Möglichkeit der Fernadministration auf dem Router-Gerät.....	67
Das Heimnetzwerk auf Abwesenheit vorbereiten.....	67
Geräte neu starten oder gezielt ausschalten gehört zum guten Ton!.....	68
Verdacht auf einen erfolgreichen Angriff.....	68
Kompromittierter Router.....	69
Kompromittierter Router oder Malware.....	69
Malware.....	69
Ransomware.....	71
Kompromittierter Account.....	71
Mögliche Beseitigungen von Bedrohungen in einem kompromittierten persönlichen Netzwerk.....	72
Kompromittierter Router.....	72
Malware (z. B. Spyware, Adware, Rootkits).....	72
Ransomware.....	72
Kompromittiertes Konto.....	73
Aggressive Beseitigung von Bedrohungen in einem gefährdeten persönlichen Netzwerk.....	73
Alle Geräte vom Netzwerk trennen und Netzwerkgeräte zurücksetzen.....	73
Werkseinstellungen auf zuvor verbundenen Geräten durchführen.....	74
Sofortige Passwortänderung und erforderliches erneutes Einloggen von allen verbundenen Geräten.....	74
Persönliche Netzwerke und Daten schützen.....	74

Kapitel 4

Das Tor zum Internet: Browser, aber sicher.....	75
Sichere Verbindungen im Browser.....	77
Wo Vorsicht geboten ist.....	78
Plug-ins zur Erhöhung der Sicherheit.....	79
Privatsphäre.....	79
Browserwahl.....	79
Privater Modus.....	80
Cookie- und Trackerblocking.....	81
Plug-ins.....	82
Tracking in Mails.....	83
Das Darknet.....	85
DNS-Server ändern für mehr Privatsphäre.....	89

Kapitel 5

Sichere Bankgeschäfte im Internet.....	91
Einführung in das Online-Banking.....	91
Basics für sicheres Online-Banking.....	92
Risiken bei der Geldverwaltung aus der Ferne.....	93





Inhaltsverzeichnis 13

Grundlegende Sicherheitsmaßnahmen einhalten.....	94
Banking-Apps – Fluch oder Segen?.....	96
Ihr Notfallplan: Das ist bei einem Betrug sofort zu tun!.....	96

Kapitel 6

Kein Backup — kein Mitleid. So sichern Sie Ihre Daten richtig.....

99

Warum sind Backups wichtig?.....	99
Schutz vor Hardwareausfällen.....	100
Schutz vor menschlichen Fehlern.....	100
Schutz vor Malware und Ransomware.....	101
Schutz vor Naturkatastrophen.....	101
Großbrand legt Cloud lahm.....	101
Erste Bilanz der Schäden nach dem Großbrand.....	101
Die Bedeutung von Backups.....	102
Verschiedene Datensicherungsmethoden.....	103
Vollbackup.....	103
Differenzielles Backup.....	103
Inkrementelles Backup.....	103
Die 3-2-1-Backup-Regel.....	104
Backups von Mobilgeräten.....	105
iOS-Geräte.....	105
Android-Geräte.....	105
Backups sind nicht kostenlos.....	106
Beispielhafte Lösung: Duplicati.....	106
Mit Bordmitteln auf macOS ein Backup anlegen.....	108
Mit Bordmitteln auf Windows eine Sicherung der Einstellungen anlegen.....	111
Mit Bordmitteln auf Windows einen Wiederherstellungspunkt anlegen.....	112

Kapitel 7

Ihre Informationen in fremden Händen — Datenlecks.....

119

Abfluss von Daten – die Langzeitnachwirkungen.....	120
Arten von Datenlecks – absichtliche und unabsichtliche.....	121
Innentäter und Whistleblower.....	122
Der externe Täter.....	124
Anzeichen, dass Sie das Opfer eines Datenlecks geworden sind.....	125
Setzen Sie Ihr Bauchgefühl ein.....	125
Identity Leak Checker: für mehr Gewissheit.....	125
Have I been pwned: letzte Zweifel aus dem Weg räumen.....	127
HIBP ist Open Source.....	129
Daten gestohlen? So reagieren Sie jetzt richtig!.....	129
Datenlecks – die richtige Prävention.....	130
Nutzen Sie Felder, um Hinweise zu hinterlassen.....	131
Beliebig viele E-Mail-Adressen dank des Pluszeichens.....	131



14 Inhaltsverzeichnis

Private-Relay und E-Mail-Adresse verbergen.....	132
Digitalen Fußabdruck reduzieren.....	132
Digitale Hygiene betreiben.....	133
Datenschutzbehörden und Ihre Rechte.....	134
Die DSGVO – Ihr schärfstes Schwert.....	134

Kapitel 8

Endlich Endgeräte absichern und schützen 139

Bedrohungen für Computersysteme	139
Malware	140
Man-in-the-Middle-Angriffe.....	140
Zero-Day-Exploits	142
Allgemeine Bedrohungen für die Systemsicherheit.....	143
Fakt oder Mythos: Ransomware auf dem Mac?.....	145
macOS-Sicherheit.....	147
Windows-Sicherheit.....	148
Mobile Endgeräte absichern.....	149
Bluetooth ausschalten	149
Starke PINs/Passwörter verwenden	150
Öffentliches WLAN meiden:	150
Physische Kontrolle beibehalten.....	151
Mikrofon und Kamera abschirmen	151
Vorsicht bei der Installation von Anwendungen	151
Updates durchführen.....	152
Biometrische Authentifizierung nutzen	153
Vorsicht bei E-Mail-Anhängen und Links.....	153
Ortungsdienste deaktivieren.....	153
Regelmäßiger Neustart	154
Jailbreaking oder Rooting vermeiden	154
Original-Ladezubehör verwenden.....	155

TEIL II

DER MENSCH IM FOKUS..... 157

Kapitel 9

Menschliche Sicherheit..... 159

Der menschliche Faktor als Sicherheitsrisiko.....	159
Der menschliche Faktor als Schlüssel zur Verbesserung der Sicherheit	160
Gefährliche Selbstgefälligkeit.....	160
Was versteht man unter Selbstgefälligkeit?.....	161
Warum ist Selbstgefälligkeit so riskant?.....	161
Häufige Verbesserungspotenziale.....	161
Klicken auf schädliche Links.....	162
Verwendung schwacher Passwörter	162
Übersehen von Sicherheitsupdates	162

Inhaltsverzeichnis 15

Social Engineering und menschliches Verhalten	163
Pretexting	163
Tailgating	163
Shoulder Surfing.....	164
Sicherheitsbewusstsein und Schulung.....	166
Open Source Intelligence und Oversharing.....	167
Sechs Kategorien von OSINT-Informationen.....	167
Clean Desk Policy.....	168
Wie Sie mit einer Clean Desk Policy beginnen.....	168
Security Awareness: Warum traditionelle Ansätze häufig scheitern und wie die Security Awareness Curve Abhilfe schafft.....	169
Die Problematik des derzeitigen Sicherheitsbewusstseins.....	169
Was ist die Security Awareness Curve?.....	169
Inwiefern kann die Security Awareness Curve helfen?.....	170
Rolle der Nutzererfahrung (UX) in der digitalen Sicherheit.....	171
UX und digitale Sicherheit.....	171
Ethik und Verantwortung: Ein Blick auf digitale Sicherheit.....	172
Ethik in der digitalen Sicherheit.....	172
Datenschutz und Privatsphäre.....	173
Fallstudien: Der menschliche Faktor in der digitalen Sicherheit.....	173
Eine Sicherheitsverletzung durch Phishing.....	173
Verbesserung der digitalen Sicherheit durch bewusste Praktiken.....	174
Zukünftige Herausforderungen.....	174
Aufkommende Technologien.....	174
Sich verändernde Arbeitsmodelle.....	175

Kapitel 10

Phishing-Mails — so erkennen Sie die falsche Nachricht..... 177

Phishing — bewährte Tradition von Kriminellen.....	177
Das Sender Policy Framework (SPF) im Kontext von E-Mail-Sicherheit verstehen	178
DomainKeys Identified Mail (DKIM) Protocol für E-Mail-Sicherheit.....	179
Entwicklung und Funktion von DMARC.....	180
Der Wurm muss dem Fisch schmecken — erkennen Sie den Köder	182
Tarnung der Phishing-E-Mails.....	182
Speerfische und wie Sie die Meerbewohner auf Distanz halten.....	185
Ein gesundes Maß an Skepsis	185
Ihr Verstand – die beste und schlechteste Waffe	186
Die Top-3-Betreffzeilen für Phishing-Angriffe.....	187
Die Gefahr von Phishing.....	188
Neue Grenzen durch innovative Methoden?	188
Phishing 4.0 — künstliche Intelligenz als Gamechanger.....	189



16 Inhaltsverzeichnis

Kapitel 11

Vishing, Smishing, Chishing — die Familie

Phishing wird größer	191
Smishing.....	191
Empfehlungen zur Vermeidung von Smishing-Angriffen	192
Vishing.....	192
Ping-Call —nah am Vishing und doch nicht das Gleiche	194
Schutzmaßnahmen.....	194
Chishing – Phishing im Chat	194
Phishing über Google Docs: eine detaillierte Betrachtung.....	195

Kapitel 12

Ransomware — wenn der Rechner nur noch

kryptisch spricht.....	197
Ransomware entmystifiziert: Geschichte, Funktionsweise und Herausforderung.....	197
Bedeutende Angriffe: WannaCry und Emotet.....	200
Die Auswirkungen von Ransomware: persönliche und finanzielle Konsequenzen.....	200
Folgen eines Identitätsdiebstahls.....	201
Infektionswege: So kommt der Schädling auf Ihr System	203
Schutz vor Ransomware: Das Immunsystem Ihres Systems	203
Präventive Maßnahmen zur Sicherung des Systems	204
Die Wichtigkeit von Backups: die Lebensversicherung für Ihre Daten	204
Ransomware auf dem Mac	205
Notfall: Das ist zu tun, wenn Sie sich infiziert haben!.....	206
Suchen Sie nach einer Readme-Datei.....	206
Trennen Sie Ihr Gerät vom Internet.....	207

TEIL III

LUG UND BETRUG IM INTERNET..... 209

Kapitel 13

Die Evergreens: Diese Betrugsmaschen gibt es

schon ewig.....	211
Der Klassiker: Mit Phishing geben Kriminelle vor jemand zu sein, der sie nicht sind!	212
Erst geben, dann nehmen. Sie geben und der Kriminelle nimmt!.....	213
Die falschen Mitarbeiter am Telefon!.....	213
Die Liebe im Internet. Ist nicht immer echt!.....	214
In letzter Minute das Angebot bekommen und Geld verloren!.....	215
Der Traumjob ist nur einen Klick entfernt. Nicht.....	216
Kriminelle schaffen eine Situation, um Sie zu erpressen	216
Wenn das Finanzamt sich meldet. Und Sie nicht drangehen!.....	217



Kapitel 14	
One-Hit-Wonder: Auf diese Maschen fallen Sie garantiert nur einmal herein	219
Der Betrug per Vorkasse	219
Der falsche Verwandte	220
Die nicht existierende Wohltätigkeitsorganisation	223
Der unseriöse Handwerker	224
Der einzige Shop mit Produkten	226
Kapitel 15	
Die Newcomer: Neue Technologien schaffen neue Betrugsmaschen	227
Einführung in neue Technologien und Betrug	227
Historischer Kontext von Technologie und Betrug	228
Sextortion-Mails	229
Künstliche Intelligenz und digitale Sicherheit	231
Künstliche Intelligenz und Deepfakes	232
Was sind Deepfakes?	232
Das Internet der (unsicheren) Dinge?	233
Blockchain und Kryptowährungsbetrug	235
Betrugserkennung in neuen Technologien	238
Maschinelles Lernen zur Betrugserkennung	238
Common Practices für den Umgang mit neuen Technologien	238
Zukunft von Betrug und neuen Technologien	239
Deepfakes und künstliche Intelligenz	239
Internet der Dinge (IoT)	239
Kryptowährung und Blockchain-Betrug	240
Cyber-Angriffe auf kritische Infrastrukturen	240
Kapitel 16	
So bereiten Sie sich auf eine Ausnahmesituation vor	241
Warum ein Notfallplan wichtig ist	241
Was wollen die Angreifer?	241
Sofortmaßnahmen beim Verdacht auf eine Infektion mit Schadsoftware	242
Suchen Sie nach einer Readme-Datei	242
Trennen Sie Ihr Gerät vom Internet	242
Vorbereitet zu sein, ist entscheidend	242
Inhalte für KMUs auch für Privatpersonen sinnvoll	244
Das IT-Notfall-Paket	244



18 Inhaltsverzeichnis

TEIL IV	
DER TOP-TEN-TEIL	245
Kapitel 17	
Die 10 Tipps für ein sicheres Internet zu Hause	247
Priorisieren Sie Ihre Passwörter!	247
Nur so viel Software wie nötig, stets aktuell!	247
Behalten Sie persönliche Daten für sich!	248
Seien Sie auf das Schlimmste vorbereitet — Backup erstellen und sich sicher fühlen!	249
Lassen Sie einen Wächter auf Ihr System achten — installieren Sie Antivirensoftware!	249
Bösartige Mails erkennen und Angriffe vermeiden — schließen Sie die Tür vor Angreifern!	250
Halten Sie Abstand von ungesicherten Websites	251
Vermeiden Sie öffentliche, ungesicherte Netzwerke	251
Überprüfen und aktualisieren Sie regelmäßig Ihre Einstellungen	251
Nutzen Sie ein Virtual Private Network (VPN) für mehr Sicherheit unterwegs!	252
Kapitel 18	
Die Top 10 Betrugsmaschen	255
Ware existiert nicht, wird aber trotzdem verkauft	255
Wie schützen Sie sich?	255
Der Dreiecksbetrug — Vorsicht, schwer durchschaubar	256
Wie schützen Sie sich?	256
Die Stellenanzeige — zu verlockend? Vorsicht ist geboten	256
Wie schützen Sie sich?	257
Romance Scamming — wenn die digitale Liebe nicht echt ist	257
Wie kann ich mich schützen?	258
Paketbetrug per SMS — ein Klick vom Betrüger entfernt	258
Wie kann ich mich schützen?	259
Einsammeln von Daten — besser nicht ins Netz laufen	259
Wie kann ich mich schützen?	260
Windows-Updates — Return of the Suchleiste	260
Wie kann ich mich schützen?	260
Erpressung in allen Formen und Varianten	260
Wie schütze ich mich?	261
Gutscheinbetrug — tausche Plastik gegen Geld	261
Wie kann ich mich schützen?	262
Vorschussbetrug — wenn Geld erst gegen Geld fließt	262
Wie kann ich mich schützen?	262



Inhaltsverzeichnis 19

Kapitel 19	
Die Top 10 Tipps im Internet.....	263
Anpassung und Aktualisierung des Webbrowsers.....	263
Schutz Ihrer Daten durch Verschlüsselung.....	263
Erstellung regelmäßiger Sicherungskopien.....	263
Einsatz eines Werbeblockers.....	264
Vorsicht bei E-Mails und ihren Anhängen.....	264
Vorsicht bei Downloads, insbesondere von Programmen.....	264
Zurückhaltung bei der Weitergabe persönlicher Daten.....	265
Schutz Ihrer Online- und Benutzerkonten durch sichere Passwörter.....	265
Erstellung unterschiedlicher Benutzerkonten.....	265
Aktualisierung des Betriebssystems und anderer Software.....	266
 Kapitel 20	
Die Top 10 prominenten Datenlecks und was Sie daraus	
lernen können.....	267
Der-Facebook-Datenleak: 500 Millionen Betroffene!.....	267
iCloud-Fotoleak: Sensibler geht nimmer!.....	268
Fremdgehplattform Ashley Madison. Auweia!.....	269
Equifax — Angriff auf US-Schufa.....	272
Freedom Hosting II — auch im Darknet ist nichts vor Hackern sicher!.....	273
Knuddels Hack im September 2018 — die erste Strafe nach DSGVO.....	273
LinkedIn — Datendiebstahl und eingesammelte Daten im großen Stil.....	274
Snapchat — Daten vieler Minderjähriger enthalten.....	275
Twitter — soziale Netzwerke sind ein beliebtes Ziel.....	276
Den Schluss macht der Anfang — MySpace im Jahr 2008!.....	277
 Abbildungsverzeichnis.....	279
Stichwortverzeichnis.....	285

