

# Inhaltsverzeichnis

## 1. Sicherheits-Checklisten..... 13

1.1	Windows.....	13
1.2	Android.....	13
1.3	iOS.....	14
1.4	Webbrowser.....	14
1.5	Onlineshopping & -banking.....	15
1.6	Passwörter.....	15
1.7	Internet- und WLAN-Router.....	15
1.8	NAS & Co.....	16
1.9	Cloud-Dienste.....	16

## 2. Das A und O: sichere Passwörter..... 17

2.1	Wurde einer Ihrer Onlinezugänge schon gehackt?.....	17
2.2	Sofortmaßnahmen im Ernstfall.....	18
	Symptome für gehackte Passwörter.....	18
	Sofort Gegenmaßnahmen ergreifen.....	20
2.3	Zuverlässige Passwörter wählen.....	21
	Was steht auf dem Spiel?.....	22
	Wie sicher ist mein Passwort?.....	22
	So werden Passwörter sicher.....	23
	Wie lang sollte ein gutes Passwort sein?.....	24
	Passwörter schützen.....	25
	Ein sicheres Passwort generieren.....	27
2.4	Hacking-Workshop: Passwörter knacken.....	29
	Archive mit Passwortschutz erstellen.....	29
	Geschützte Archive hacken.....	31
2.5	Passwort-Manager für Schutz mit Komfort.....	36
	KeePass in Betrieb nehmen.....	37
	Zugangsdaten in KeePass speichern.....	41
	KeePass im Browser verwenden.....	51
	KeePass auf Mobilgeräten.....	56

2.6	Zwei-Faktor-Authentifizierung (2FA) .....	61
	Zwei-Faktor-Anmeldungen bei Onlinediensten.....	62
	2FA bei Google-Konten ohne App.....	65
	2FA mit Authy.....	67
2.7	FIDO2 statt Passworteingabe.....	73
	FIDO2 schon heute praktisch nutzen .....	73

### 3. Windows-PC: Zugang und Daten schützen ..... 77

3.1	Sperrbildschirm und Anmeldeoptionen .....	77
	Die Anmeldevarianten bei Windows 10 .....	77
	Nur ausgewählte Informationen auf dem Sperrbildschirm .....	82
	Hacking-Workshop: Windows-Anmeldung knacken.....	83
3.2	Windows-Benutzerkonten sinnvoll einsetzen.....	85
	Zusätzliche Konten für weitere Benutzer anlegen.....	86
	Das Kennwort eines Benutzerkontos ändern .....	88
	Kontoname und Kontotyp nachträglich verändern.....	91
3.3	Benutzerkontensteuerung schützt PC und Daten.....	92
	Die Berechtigungsstufen der Benutzerkontensteuerung.....	93
	Die Privilegien des Administratorkontos.....	94
	Sichere Hausmannskost als Standardbenutzer .....	95
	Die Benutzerkontensteuerung anpassen .....	96
3.4	Windows stets auf dem aktuellen Stand .....	102
	Hacking-Workshop: Windows mit dem Hacker-Baukasten angreifen.....	102
	Vollautomatische Windows-Updates .....	106
	Mehr Kontrolle: den Update-Zeitraum selbst bestimmen.....	108
	Installierte Updates überprüfen .....	109
	Updates bei Problemen mittels Rollback rückgängig machen.....	110
3.5	Software in der Windows-Sandbox testen .....	112
	Die Sandbox-Funktion aktivieren .....	112
	Windows-Sandbox ausführen und nutzen.....	113
	Die Windows-Sandbox konfigurieren .....	115
3.6	Dateien verschlüsseln .....	116
	Ausgewählte Dateien und Ordner schützen.....	117
	Komplette Laufwerke verschlüsseln .....	121

	Daten auf USB-Sticks und Speicherkarten schützen.....	130
	VeraCrypt: kostenlose und sichere Alternative.....	134
3.7	Windows-PCs im Netzwerk schützen .....	139
	Öffentliche Netze nur mit aktivem Schutzschild.....	140
	Die klassische Windows Defender Firewall für zuverlässigen Basisschutz.....	141
	Erweiterte Firewall-Einstellungen für flexiblen Schutz.....	146

## 4. Android-Geräte sicher nutzen ..... 151

4.1	Den Zugang zum Gerät kontrollieren .....	151
	Passwörter bei der Eingabe zuverlässig verbergen.....	154
	Anmelden per Wischmuster .....	154
	Per Fingerabdruck entsperren .....	156
	Smart Lock – Sperren nur, wenn nötig.....	158
4.2	Ein Android-Gerät sicher mit anderen teilen .....	160
	Weitere Benutzer anlegen .....	160
	Zwischen Benutzerkonten wechseln.....	161
4.3	Android aktuell halten – wenn möglich .....	162
	Keine Updates mehr? Alternativen prüfen.....	163
	Apps aktuell halten .....	165
4.4	Apps sicher installieren und kontrollieren.....	166
	Android-Apps – darauf sollten Sie achten .....	166
	Software aus anderen Quellen installieren .....	168
	Berechtigungen für Apps prüfen und beschränken .....	169
	Apps als Geräteadministratoren.....	171
	Apps als Bedienhilfen.....	172
4.5	Virenschutz für Android-Geräte.....	173
	So reagiert Play Protect auf problematische Apps .....	174
4.6	Daten auf Android-Geräten verschlüsseln.....	175
	Die Geräteverschlüsselung aktivieren.....	176
4.7	Geräte bei Verlust aufspüren oder sperren.....	178
	Fernzugriff auf Android-Geräte .....	178
4.8	Root-Zugriff: mehr Schaden als Nutzen? .....	180
	Das spricht gegen Root-Zugriff .....	180

## 5. iPhone und iPad: iOS mit Sicherheit ..... 183

5.1	Das Gerät sicher und komfortabel sperren .....	183
	Per Biometrie entsperren.....	184
	Biometrie für weitere Autorisierungen verwenden .....	185
	Was wird bei gesperrtem Gerät preisgegeben? .....	186
5.2	iOS aktuell halten .....	186
	Neue Updates automatisch einspielen .....	187
5.3	App-Berechtigungen kontrollieren .....	188
	Welche Berechtigung hat eine bestimmte App? .....	189
5.4	Das Gerät im Verlustfall orten und sperren .....	189
5.5	Zwei-Faktor-Authentifizierung für die Apple-ID.....	191
5.6	Sichere Backups für den Ernstfall .....	192
	Verschlüsselte Komplett-Backups mit iTunes.....	193

## 6. Drahtlos sicher: WLANs ohne Risiko ..... 195

6.1	Das eigene WLAN zuverlässig absichern.....	195
	Eigener Name für das Drahtlosnetzwerk .....	197
	Kennwort und Verschlüsselung optimal wählen .....	199
	Zugangsteuerung per MAC-Adresse .....	202
	Sicherheitslücke: WLAN-Geräte per WPS anmelden.....	206
6.2	Besuchern ein Gäste-WLAN gefahrlos bereitstellen .....	208
	Privates Gäste-WLAN einrichten .....	209
	QR-Code für schnelles, unkompliziertes Anmelden ausdrucken .....	211
	Den Gästezugang mit Filterregeln flexibel steuern.....	212
6.3	Fremde Netzwerke ohne Risiken nutzen .....	214
	Gefahrenquelle öffentliche Hotspots .....	214
	Gefahrenquelle Hotspot-Portalseiten .....	218
	Mit VPN überall sicher online gehen.....	220

## 7. Malware: Viren & Co. vermeiden & bekämpfen ..... 233

7.1	Verhaltensregeln: Schädlinge vermeiden.....	233
	Fremde Speichermedien prüfen .....	233
	Vorsicht bei E-Mail-Anhängen.....	234

	Datei-Downloads .....	235
	Drive-By-Infektionen .....	237
7.2	Infektionen mit Antivirensoftware verhindern .....	238
	Funktioniert mein Virenschutz? .....	238
	Den PC mit Windows Defender schützen .....	240
7.3	Erpressungstrojaner .....	250
	Schutz vor Erpressungstrojanern .....	251
	Sofortmaßnahmen.....	254
	Den Übeltäter sicher identifizieren .....	255
	Den Schädling loswerden.....	257
	Die Dateiverschlüsselung aufheben .....	264
7.4	Verdächtige Datei mit Sysinternal-Tools analysieren.....	268
	Sysinternals-Tools im Explorer bereitstellen .....	269
	Alle Autostart-Einträge gründlich prüfen .....	271
	Verdächtige Anwendungen mit dem Prozess-Explorer erkennen.....	272
	Programme mit dem Prozessmonitor analysieren .....	276

## **8. Web und Cloud gefahrlos nutzen..... 279**

8.1	Webbrowser aktuell halten .....	279
	Firefox aktualisieren .....	279
	Chrome aktualisieren .....	280
8.2	Sichere Webseiten mit HTTPS .....	281
	Die Sicherheit einer Webseite prüfen.....	283
	Mit HTTPS Everywhere überall sicher surfen .....	284
8.3	Angriffe über aktive Inhalte vermeiden.....	287
	Hacking-Workshop: Sind Seiten per Clickjacking verwundbar?.....	288
	JavaScript deaktivieren.....	290
	Inhalte mit NoScript gezielt steuern.....	292
8.4	Sicherheitsrisiko Browser-Erweiterungen und -Plug-ins.....	295
	Vor dem Installieren prüfen .....	295
	Vorhandene Erweiterungen kontrollieren.....	296
	Plug-ins für zusätzliche Webtechnologien .....	298
8.5	Webseitenberechtigungen kontrollieren.....	299
	Berechtigungen kontrollieren und nachträglich ändern .....	300

	Alle Berechtigungen einer bestimmten Webseite betrachten.....	301
	Berechtigungen nur in Ausnahmefällen erteilen.....	302
8.6	Sichere Passwörter für Webdienste.....	303
	Anmelden als?.....	304
	Passwort-Manager im Webbrowser? .....	304
8.7	Onlineshopping.....	305
	Zuverlässige Onlinehändler.....	306
	Online sicher bezahlen .....	309
	Kaufvertrag sicher abschließen .....	311
	One-Touch-Shopping – pro und kontra .....	312
	Sonderfall Onlineauktionen und -kleinanzeigen .....	313
8.8	Onlinebanking .....	314
	Mehrfacher Schutz fürs Onlinebanking.....	315
	Onlinebanking ohne Datenspuren .....	315
	Banking per App .....	316
8.9	Cloud-Dienste sicher nutzen .....	317
	Zwei-Faktor-Authentifizierung nutzen .....	318
	Angemeldete Geräte überprüfen .....	321
	App-Freigaben kontrollieren .....	322
	Boxcryptor: Daten verschlüsselt in der Cloud speichern.....	323

## **9. Heimnetzwerk und Geräte schützen ..... 329**

9.1	Web- und Wartungszugänge absichern.....	329
	Eigene Zugangsdaten verwenden .....	330
	Fernzugriffe und -wartung abschalten .....	331
	Wichtige Änderungen zusätzlich bestätigen .....	334
	Die Tastensperre der FRITZ!Box aktivieren.....	334
9.2	Firmware aktualisieren .....	335
9.3	Portfreigaben kontrollieren und absichern.....	337
	Hacking-Workshop: Schwachstellen per Portscan aufspüren.....	338
	Portscan am eigenen Internetanschluss .....	340
	Portfreigaben im Router steuern .....	342
	Sicherheitsfalle UPnP.....	345
	Ein Gerät komplett für den Zugriff freigeben (DMZ) .....	348

9.4	Nur notwendige Funktionen eingeschaltet lassen.....	348
	Erweiterte Ansicht für volle Kontrolle .....	349
9.5	Nachricht bei Problemen oder Verdacht.....	350
	Worüber soll wie benachrichtigt werden?.....	351
9.6	Besondere Maßnahmen bei NAS .....	351
	Zusatzpakete bei NAS kontrollieren .....	352
	Pakete auf dem aktuellen Stand halten.....	353
	Verschlüsselter Zugriff aufs NAS.....	354
	Ordner mit wichtigen Daten verschlüsseln.....	356

<b>Stichwortverzeichnis .....</b>	<b>359</b>
-----------------------------------	------------