Bitdefender®

# TOTAL SECURITY MULTI-DEVICE 2018

BENUTZERHANDBUCH

# Bitdefender Total Security Multi-Device 2018
# **Benutzerhandbuch**

Veröffentlicht 10.06.2018

Copyright© 2018 Bitdefender

## Rechtlicher Hinweis

Alle Rechte vorbehalten. Bestandteile dieses Handbuches dürfen weder in elektronischer noch mechanischer Form reproduziert werden. Dies gilt auch für das Fotokopieren, Aufnehmen oder jegliche andere Form von Datenspeicherung oder Informationsbeschaffung, ohne die Zustimmung von Bitdefender. Ausnahmen gelten für Zitate in Verbindung mit Testberichten. Der Inhalt darf in keiner Weise verändert werden.

**Warnung und Haftungsausschluss.** Dieses Produkt und die dazugehörige Dokumentation sind urheberrechtlich geschützt. Die Informationen in diesem Dokument werden „ohne Mängelgewähr" gegeben. Obwohl dieses Dokument mit äußerster Sorgfalt erstellt und geprüft wurde, übernehmen die Autoren keinerlei Haftung für tatsächlich oder angeblich auftretende Schäden bzw. Datenverluste, die direkt oder indirekt durch die Informationen in diesem Dokument entstehen könnten oder bereits entstanden sind.

Dieses Handbuch enthält Verweise auf andere, nicht von Bitdefender erstellte oder von Bitdefender kontrollierte Webseiten und somit übernimmt Bitdefender auch keine Verantwortung für die Inhalte dieser Webseiten. Der Besuch der in diesem Dokument aufgelisteten Drittanbieter-Webseiten erfolgt damit auf eigene Gefahr. Bitdefender stellt diese Links der Einfachheit zur Verfügung. Dies bedeutet nicht, dass Bitdefender den Inhalt einer Website Dritter befürwortet oder Verantwortung dafür übernimmt.

**Warenzeichen.** Es erscheinen eingetragene Warenzeichen in diesem Dokument. Alle eingetragenen und nicht eingetragenen Warenzeichen in diesem Dokument sind das alleinige Eigentum der jeweiligen Besitzer.

Bitdefender

# Inhaltsverzeichnis

Über diese Anleitung ..... x
1. Zielsetzung und Zielgruppe ..... x
2. Über dieses Handbuch ..... x

Total Security für PC ..... 1

1. Installation ..... 2
1.1. Vor der Installation ..... 2
1.2. Systemanforderungen ..... 2
1.3. Installieren Ihres Bitdefender-Produkts ..... 4

2. Inbetriebnahme ..... 12
2.1. Grundlagen ..... 12
2.1.1. Probleme beheben ..... 14
2.1.2. Nachrichten ..... 16
2.1.3. Autopilot ..... 17
2.1.4. Profile ..... 18
2.1.5. Passwortschutz für Bitdefender-Einstellungen ..... 19
2.1.6. Anonyme Nutzungsberichte ..... 20
2.1.7. Benachrichtigungen zu Sonderangeboten ..... 21
2.2. Bitdefender-Benutzeroberfläche ..... 21
2.2.1. Task-Leisten-Symbol ..... 22
2.2.2. Hauptfenster ..... 23
2.2.3. Die Bitdefender-Bereiche ..... 27
2.2.4. Sicherheits-Widget ..... 32
2.2.5. Aktivität ..... 34
2.3. Bitdefender Central ..... 38
2.3.1. Meine Abonnements ..... 39
2.3.2. Meine Geräte ..... 41
2.3.3. Aktivität ..... 44
2.3.4. Mein Konto ..... 45
2.3.5. Nachrichten ..... 46
2.4. Bitdefender auf dem neuesten Stand halten ..... 46
2.4.1. Überprüfen, ob Bitdefender auf dem neuesten Stand ist ..... 47
2.4.2. Durchführung eines Updates ..... 47
2.4.3. Aktivieren / Deaktivieren der automatischen Updates ..... 48
2.4.4. Update-Einstellungen anpassen ..... 49
2.4.5. Regelmäßige Updates ..... 50

3. Gewusst wie ..... 51
3.1. Installation ..... 51
3.1.1. Wie installiere ich Bitdefender auf einem zweiten Computer? ..... 51
3.1.2. Wie kann ich Bitdefender neu installieren? ..... 51
3.1.3. Wo kann ich mein Bitdefender-Produkt herunterladen? ..... 53
3.1.4. Wie kann ich die Sprache für mein Bitdefender ändern? ..... 53
3.1.5. Wie verfahre ich mit meinem Bitdefender-Abonnement nach einem Windows-Upgrade? ..... 55

3.1.6. Wie kann ich ein Upgrade auf die neueste Bitdefender-Version durchführen? . . . 58
3.2. Abonnements . . . 59
3.2.1. Wie kann ich mein Bitdefender-Abonnement mithilfe eines Lizenzschlüssels aktivieren? . . . 59
3.3. Bitdefender Central . . . 60
3.3.1. Wie melde ich mit einem anderen Benutzerkonto bei Bitdefender Central an? . . . 60
3.3.2. Wie kann ich die Bitdefender Central-Hilfemeldungen deaktivieren? . . . 60
3.3.3. Ich habe das Passwort vergessen, das ich für mein Bitdefender-Konto festgelegt habe. Wie kann ich es zurücksetzen? . . . 61
3.3.4. Wie kann ich die Benutzersitzungen in meinem Bitdefender-Konto verwalten? . . . 62
3.4. Prüfen mit Bitdefender . . . 62
3.4.1. Wie kann ich eine Datei oder einen Ordner scannen? . . . 62
3.4.2. Wie scanne ich mein System? . . . 63
3.4.3. Wie plane ich einen Scan? . . . 63
3.4.4. Wie kann ich eine benutzerdefinierte Scan-Aufgabe anlegen? . . . 64
3.4.5. Wie kann ich einen Ordner vom Scan ausnehmen? . . . 65
3.4.6. Wie gehe ich vor, wenn Bitdefender eine saubere Datei als infiziert eingestuft hat? . . . 66
3.4.7. Wo sehe ich, welche Bedrohungen Bitdefender gefunden hat? . . . 67
3.5. Elternberater . . . 68
3.5.1. Wie kann ich meine Kinder vor Bedrohungen aus dem Internet schützen? . . . 68
3.5.2. Wie hindere ich mein Kind daran, eine bestimmte Website aufzurufen? . . . 69
3.5.3. Wie verhindere ich, dass mein Kind ein bestimmtes Spiel spielt? . . . 70
3.5.4. Wie kann ich verhindern, dass mein Kind mit nicht vertrauenswürdigen Menschen in Kontakt kommt? . . . 70
3.5.5. Wie kann ich einen Ort als sichere oder unsichere Zone für mein Kind festlegen? . . . 72
3.5.6. Wie blockiere ich an Schultagen den Zugang meines Kindes zu den ausgewählten Geräten? . . . 74
3.5.7. Wie blockiere ich an Schultagen abends den Zugang meines Kindes zu den ausgewählten Geräten? . . . 73
3.5.8. Wie blockiere ich am Wochenende den Zugang meines Kindes zu den ausgewählten Geräten? . . . 74
3.5.9. Wie entferne ich das Profil für mein Kind? . . . 75
3.6. Privatshpäreschutz . . . 75
3.6.1. Wie sichere ich meine Online-Transaktionen ab? . . . 75
3.6.2. Was kann ich tun, wenn mein Gerät gestohlen wurde? . . . 76
3.6.3. Wie benutze ich einen Datentresor? . . . 76
3.6.4. Wie lösche ich mit Bitdefender eine Datei unwiderruflich? . . . 78
3.6.5. Wie schütze ich meine Webcam vor Hackern? . . . 79
3.7. Optimierungstools . . . 79
3.7.1. Wie verbessere ich die Leistung meines Systems? . . . 79
3.7.2. Wie kann ich meine Systemstartzeit verbessern? . . . 81
3.8. Nützliche Informationen . . . 81
3.8.1. Wie kann ich meine Sicherheitslösung selbst testen? . . . 81
3.8.2. Wie kann ich Bitdefender entfernen? . . . 82

3.8.3. Wie kann ich Bitdefender VPN entfernen? . . . 83
3.8.4. Wie fahre ich den Computer automatisch herunter, nachdem der Scan beendet wurde? . . . 84
3.8.5. Wie konfiguriere ich Bitdefender für die Nutzung einer Proxy-Verbindung? . . . 85
3.8.6. Ist auf meinem System die 32- oder 64-Bit-Version von Windows installiert? . . . 86
3.8.7. Wie kann ich in Windows versteckte Objekte anzeigen? . . . 87
3.8.8. Wie entferne ich andere Sicherheitslösungen? . . . 87
3.8.9. Wie führe ich einen Neustart im abgesicherten Modus durch? . . . 89

4. Die Sicherheitselemente im Detail . . . 91
4.1. Virenschutz . . . 91
4.1.1. Zugriff-Scans (Echtzeitschutz) . . . 92
4.1.2. Bedarf-Scan . . . 97
4.1.3. Automatischer Scan von Wechselmedien . . . 107
4.1.4. Host-Datei scannen . . . 109
4.1.5. Konfiguration der Scan-Ausschlüsse . . . 110
4.1.6. Verwalten von Dateien in Quarantäne . . . 113
4.2. Advanced Threat Defense . . . 114
4.3. Internet-Schutz . . . 116
4.4. Spam-Schutz . . . 119
4.4.1. Wie funktioniert der Spam-Schutz? . . . 120
4.4.2. Aktivieren / Deaktivieren des Spam-Schutzes . . . 121
4.4.3. Verwenden der Spam-Schutz-Symbolleiste in Ihrem Mail-Client-Fenster . . . 121
4.4.4. Konfigurieren der Freundesliste . . . 124
4.4.5. Konfigurieren der Spammerliste . . . 125
4.4.6. Konfigurieren der lokalen Spam-Schutz-Filter . . . 126
4.4.7. Konfigurieren der Cloud-Einstellungen . . . 127
4.5. Firewall . . . 128
4.5.1. Verwalten von App-Regeln . . . 129
4.5.2. Verbindungseinstellungen verwalten . . . 132
4.5.3. Konfigurieren der erweiterten Einstellungen . . . 133
4.6. Schwachstellen . . . 134
4.6.1. Scannen des Computers nach Schwachstellen . . . 135
4.6.2. Automatische Schwachstellensuche . . . 136
4.6.3. WLAN-Sicherheitsberater . . . 139
4.7. Webcam-Schutz . . . 142
4.8. Sichere Dateien . . . 145
4.8.1. Aktivieren und Deaktivieren von Sichere Dateien . . . 146
4.8.2. Schützen Sie Ihre persönlichen Dateien vor Ransomware-Angriffen. . . . 146
4.8.3. Konfiguration des App-Zugriffs . . . 147
4.8.4. Schutz beim Systemstart . . . 147
4.9. Verschlüsselung . . . 148
4.10. Passwortmanager-Schutz für Ihre Anmeldedaten . . . 154
4.11. VPN . . . 161
4.12. Sichere Online-Transaktionen mit Safepay . . . 165
4.13. Datenschutz . . . 169
4.14. Elternberater . . . 171

4.14.1. Aufrufen des Elternberaters - MEINE KINDER . . . . . 171
4.14.2. Profile Ihrer Kinder anlegen . . . . . 172
4.14.3. Konfigurieren der Elternberater-Profile . . . . . 178
4.15. Diebstahlschutz . . . . . 184
4.16. USB Immunizer . . . . . 186

5. Systemoptimierung . . . . . 188
5.1. Extras . . . . . 188
5.1.1. Optimierung der Systemgeschwindigkeit mit nur einem Klick . . . . . 188
5.1.2. Optimieren der Systemstartzeit . . . . . 189
5.1.3. Optimierung Ihrer Festplatte . . . . . 191
5.2. Profile . . . . . 192
5.2.1. Arbeitsprofil . . . . . 194
5.2.2. Filmprofil . . . . . 195
5.2.3. Spielprofil . . . . . 196
5.2.4. Öffentliches WLAN-Profil . . . . . 197
5.2.5. Akkubetriebsprofil . . . . . 198
5.2.6. Echtzeitoptimierung . . . . . 199

6. Problemlösung . . . . . 200
6.1. Verbreitete Probleme beheben . . . . . 200
6.1.1. Mein System scheint langsamer zu sein . . . . . 200
6.1.2. Der Scan startet nicht . . . . . 202
6.1.3. Ich kann eine App nicht mehr verwenden . . . . . 204
6.1.4. Wie gehe ich vor, wenn Bitdefender eine sichere Website oder Online-Anwendung blockiert? . . . . . 205
6.1.5. Wie gehe ich vor, wenn Bitdefender eine sichere Anwendung als Ransomware einstuft? . . . . . 206
6.1.6. Ich kann keine Verbindung zum Internet herstellen . . . . . 207
6.1.7. Ich kann auf ein Gerät in meinem Netzwerk nicht zugreifen . . . . . 207
6.1.8. Meine Internetverbindung ist langsam . . . . . 210
6.1.9. Wie man Bitdefender-Updates auch mit einer langsamen Internet-Verbindung durchführen kann . . . . . 211
6.1.10. Bitdefender-Dienste antworten nicht . . . . . 212
6.1.11. Der Spam-Schutz-Filter funktioniert nicht richtig . . . . . 212
6.1.12. Das automatische Einfügen funktioniert bei meiner Geldbörse nicht . . . 218
6.1.13. Entfernen von Bitdefender ist fehlgeschlagen . . . . . 219
6.1.14. Mein System fährt nach der Installation von Bitdefender nicht mehr hoch . . . . . 220
6.2. Entfernung von Bedrohungen . . . . . 223
6.2.1. Bitdefender-Rettungsmodus (Rettungsumgebung unter Windows 10) . . . 224
6.2.2. Wie gehe ich vor, wenn Bitdefender eine Bedrohung auf meinem Computer findet? . . . . . 228
6.2.3. Wie entferne ich eine Bedrohung aus einem Archiv? . . . . . 230
6.2.4. Wie entferne ich eine Bedrohung aus einem E-Mail-Archiv? . . . . . 231
6.2.5. Wie gehe ich vor, wenn ich eine Datei für gefährlich halte? . . . . . 232
6.2.6. Wobei handelt es sich bei den passwortgeschützten Dateien im Scan-Protokoll? . . . . . 232
6.2.7. Wobei handelt es sich bei den übersprungenen Objekten im Scan-Protokoll? . . . . . 233

6.2.8. Wobei handelt es sich bei den zu stark komprimierten Dateien im Scan-Protokoll? ... 233
6.2.9. Warum hat Bitdefender ein infizierte Datei automatisch gelöscht? ... 234

Antivirus für Mac ... 235

7. Installation und Deinstallation ... 236
7.1. Systemanforderungen ... 236
7.2. Installation von Bitdefender Antivirus for Mac ... 236
7.2.1. Installationsvorgang ... 237
7.3. Bitdefender Antivirus for Mac entfernen ... 241

8. Erste Schritte ... 242
8.1. Über Bitdefender Antivirus for Mac ... 242
8.2. Öffnen Sie Bitdefender Antivirus for Mac ... 242
8.3. Das Hauptfenster ... 243
8.4. Dock-Symbol der App ... 244

9. Schutz gegen bösartige Software ... 246
9.1. Empfohlene Vorgehensweisen ... 246
9.2. Ihren Mac scannen ... 247
9.3. Den Autopiloten ein- und ausschalten ... 248
9.4. Time-Machine-Schutz ... 248
9.5. Scan-Assistent ... 250
9.6. Alle beheben ... 251
9.7. Internet-Schutz ... 252
9.8. Updates ... 254
9.8.1. Benutzergesteuertes Update ... 254
9.8.2. Updates über einen Proxy Server ... 255
9.8.3. Upgrade auf eine neue Version durchführen ... 255
9.8.4. Informationen zu Bitdefender Antivirus for Mac finden ... 255

10. Einstellungen konfigurieren ... 257
10.1. Zugriff auf Einstellungen ... 257
10.2. Kontodetails ... 257
10.3. Schutzeinstellungen ... 258
10.3.1. Prüfausnahmen ... 259
10.4. Sichere Dateien ... 260
10.4.1. Verwalten von Anwendungen ... 263
10.5. Verlauf ... 263
10.6. Quarantäne ... 264

11. VPN ... 286
11.1. Über VPN ... 266
11.2. VPN installieren ... 266
11.3. Öffnen des VPN ... 267
11.4. Netzwerkkarte ... 267
11.5. Abonnements ... 287

12. Bitdefender Central ... 270
12.1. Über Bitdefender Central ... 270

12.2. So können Sie Bitdefender Central aufrufen: ... 270
12.3. Meine Abonnements ... 271
12.3.1. Abonnement aktivieren ... 271
12.3.2. Abonnement abschließen ... 272
12.4. Meine Geräte ... 272
12.4.1. Persönliche Anpassungen ... 272
12.4.2. Fernzugriffsaktionen ... 273
13. Häufig gestellte Fragen ... 275

Mobile Security für iOS ... 280

14. Worum handelt es sich bei Bitdefender Mobile Security for iOS? ... 281
15. Erste Schritte ... 282
16. VPN ... 286
16.1. Abonnements ... 287
17. Kontoschutz ... 289
18. Diebstahlschutz-Funktionen ... 291
19. Bitdefender Benutzerkonto ... 295

Mobile Security für Android ... 297

20. Sicherheitsfunktionen ... 298
21. Erste Schritte ... 299
22. Virenscanner ... 304
23. Kontoschutz ... 307
24. Internet-Schutz ... 309
25. VPN ... 311
26. Diebstahlschutz-Funktionen ... 315
27. App-Sperre ... 321
28. Berichte ... 326
29. WearON ... 327
30. Einstellungen ... 328
31. Info über ... 329
32. Bitdefender Central ... 330
33. Häufig gestellte Fragen ... 334

Kontaktieren Sie uns ..... 340
34. Hilfe anfordern ..... 341
35. Online-Ressourcen ..... 344
35.1. Bitdefender-Support-Center ..... 344
35.2. Bitdefender Support-Forum ..... 345
35.3. Das Portal HOTforSecurity ..... 345
36. Kontaktinformationen ..... 346
36.1. Kontaktadressen ..... 346
36.2. Lokale Vertriebspartner ..... 346
36.3. Bitdefender-Niederlassungen ..... 346
Glossar ..... 349

# Über diese Anleitung

## 1. Zielsetzung und Zielgruppe

Mit Ihrem Bitdefender Total Security Multi-Device 2018-Abonnement können Sie bis zu 10 verschiedene PCs, Macs, iOS und Android-Smartphones und -Tablets schützen. Die Verwaltung der geschützten Geräte erfolgt über ein Bitdefender-Benutzerkonto. Dieses Konto muss dazu mit einem aktiven Abonnement verknüpft sein.

Dieses Handbuch soll Ihnen bei der Einrichtung und Verwendung der Produkte, das in Ihrem Abonnement enthalten ist, in helfen: Bitdefender Total Security 2018, Bitdefender Antivirus for Mac, Bitdefender Mobile Security for iOS und Bitdefender Mobile Security auf Android-Geräten.

Sie erfahren, wie Sie Bitdefender auf verschiedenen Geräten konfigurieren können, um sie jederzeit vor allen Bedrohungen zu schützen.

## 2. Über dieses Handbuch

Dieses Handbuch befasst sich mit den vier in Bitdefender Total Security Multi-Device 2018 enthaltenen Produkten:

- „Total Security für PC“ (S. 1)

  Erfahren Sie, wie Sie das Produkt auf Ihren Windows-basierten PCs und Laptops Tablets verwenden.

- „Antivirus für Mac“ (S. 235)

  Erfahren Sie, wie Sie das Produkt auf Ihren Macs verwenden.

- „Mobile Security für iOS“ (S. 280)

  Erfahren Sie, wie Sie das Produkt auf Ihren iOS-basierten Smartphones und Tablets verwenden.

- „Mobile Security für Android“ (S. 297)

  Erfahren Sie, wie Sie das Produkt auf Ihren Android-basierten Smartphones und Tablets verwenden.

- „Kontaktieren Sie uns“ (S. 340)

  Erfahren Sie, wo Sie Hilfe erhalten, wenn etwas Unerwartetes eintritt.

# TOTAL SECURITY FÜR PC

# 1. INSTALLATION

## 1.1. Vor der Installation

Bevor Sie Bitdefender Total Security 2018 installieren, sollten Sie für eine reibungslose Installation sicherstellen, dass folgende Schritte durchgeführt wurden:

- Stellen Sie sicher, dass der Zielcomputer für die Bitdefender-Installation die Systemvoraussetzungen erfüllt. Wenn Ihr Computer nicht die Mindest-Systemanforderungen erfüllt, kann Bitdefender nicht installieren werden. Wird die Systemkonfiguration nachträglich verändert, kann es zu Leistungseinbußen und Stabilitätsproblemen kommen. Eine vollständige Liste der Systemanforderungen finden Sie im Kapitel *„Systemanforderungen“ (S. 236)*.
- Melden Sie sich mit einem Administrator-Konto am Computer an.
- Entfernen Sie alle anderen Sicherheitslösungen von Ihrem Computer. Sollte während des Bitdefender-Installationsvorgangs welche gefunden werden, werden Sie aufgefordert, sie zu deinstallieren. Die gleichzeitige Nutzung mehrerer Sicherheitsprogramme kann die jeweilige Funktion stören und massive Probleme auf Ihrem Computer verursachen. Windows Defender wird während der Installation deaktiviert.
- Deaktivieren oder entfernen Sie jegliche Firewall-Programme, die auf dem PC installiert sind. Die gleichzeitige Nutzung mehreren Sicherheitsprogrammen kann die jeweilige Funktion stören und massive Probleme auf Ihrem Computer verursachen. Die Windows-Firewall wird während der Installation deaktiviert.
- Ihr Computer sollte während der Installation mit dem Internet verbunden sein, selbst wenn Sie von CD oder DVD installieren. Falls neuere Versionen der Anwendungsdateien aus dem Installationspaket verfügbar sind, kann Bitdefender diese dann herunterladen und installieren.

## 1.2. Systemanforderungen

Sie können Bitdefender Total Security 2018 nur auf Computern mit den folgenden Betriebssystemen installieren.

- Windows 7 mit Service Pack 1
- Windows 8

- Windows 8.1
- Windows 10

Stellen Sie vor der Installation sicher, dass Ihr Computer die Mindestsystemanforderungen erfüllt.

### Beachten Sie

So können Sie Informationen zu Ihrem Windows-Betriebssystem und Ihrer Hardware finden:

- Rechtsklicken Sie unter **Windows 7** im Desktop auf **Arbeitsplatz** und wählen Sie **Eigenschaften** aus dem Menü.
- In **Windows 8**, finden Sie auf der Windows-Startseite den Eintrag **Computer**(z.B. durch die Eingabe von "Computer" auf der Startseite) und klicken Sie auf das entsprechende Symbol. Finden Sie unter **Windows 8.1 Dieser PC**.

  Wählen Sie im Menü unten **Eigenschaften**. Im Bereich **System** finden Sie Informationen zu Ihrem Systemtyp.
- Geben Sie unter **Windows 10 System** in das Suchfeld in der Taskleiste ein und klicken Sie auf das entsprechende Symbol. Im Bereich **System** finden Sie Informationen zu Ihrem Systemtyp.

## Mindestsystemanforderungen

- 1.5 GB verfügbarer Festplattenspeicher
- Dual-Core 1,6-GHz-Prozessor
- 1 GB Arbeitsspeicher (RAM)

## Empfohlene Systemanforderungen

- 2 GB freier Speicherplatz (davon mindestens 800 MB auf dem Systemlaufwerk)
- Intel CORE 2 Duo (2 GHz) oder gleichwertiger Prozessor
- 2 GB Arbeitsspeicher (RAM)

## Software-Anforderungen

Um Bitdefender und alle Funktionen nutzen zu können, muss Ihr Computer die folgenden Software-Anforderungen erfüllen:

- Ab Microsoft Edge 40
- Internet Explorer 10 und höher

- Mozilla Firefox 51 und höher
- Google Chrome 34 und höher
- Skype 6.3 und höher
- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Ab Mozilla Thunderbird 14

## 1.3. Installieren Ihres Bitdefender-Produkts

Sie können Bitdefender vom Installationsdatenträger installieren oder den Web-Installer verwenden, der über Bitdefender Central.

Falls Ihr Einkauf mehr als einen Computer umfasst, wiederholen Sie den Installationsvorgang und nutzen Sie das gleiche Benutzerkonto, um Ihr Produkt auf den einzelnen Computern zu aktivieren. Dabei müssen Sie das Benutzerkonto verwenden, das Ihr aktives Bitdefender-Abonnement enthält.

### Über Bitdefender Central installieren

Über Bitdefender Central können Sie das richtige Installationspaket für das von Ihnen erworbene Abonnement herunterladen. Nach Abschluss des Installationsvorgangs wird Bitdefender Total Security 2018 aktiviert.

So können Sie Bitdefender Total Security 2018 über Bitdefender Central herunterladen:

1. Rufen Sie Bitdefender Central auf.
2. Rufen Sie den Bereich **Meine Geräte** auf und klicken Sie auf **LOKALEN SCHUTZ INSTALLIEREN**.
3. Wählen Sie eine der beiden verfügbaren Optionen:
   - **HERUNTERLADEN**

     Klicken Sie auf die Schaltfläche und speichern Sie die Installationsdatei.
   - **Auf einem anderen Gerät**

     Wählen Sie **Windows** aus, um Ihr Bitdefender-Produkt herunterzuladen, und klicken Sie danach auf **FORTFAHREN**. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **ABSCHICKEN**.
4. Warten Sie, bis der Download abgeschlossen ist, und führen Sie das Installationsprogramm aus.

# Validierung der Installation

Bitdefender wird zuallererst Ihr System überprüfen, um die Installation zu bestätigen.

Wenn Ihr System die Mindestanforderungen zur Installation von Bitdefender nicht erfüllt, werden Sie darüber informiert, welche Bereiche aufgerüstet werden müssen, damit Sie fortfahren können.

Wenn eine inkompatible Sicherheitslösung oder eine ältere Version von Bitdefender erkannt wird, werden Sie aufgefordert, diese von Ihrem System zu entfernen. Bitte folgen Sie den Anweisungen, um die Software von Ihrem System zu entfernen und so spätere Probleme zu vermeiden. Unter Umständen müssen Sie Ihren Computer neu starten, um die Entfernung der erkannten Sicherheitslösungen abzuschließen.

Das Installationspaket für Bitdefender Total Security 2018 wird ständig aktualisiert.

**Beachten Sie**
Das Herunterladen der Installationsdateien kann eine Weile dauern, besonders bei langsameren Internetverbindungen.

Sobald die Installation validiert ist, startet der Installationsassistent. Folgen Sie den Schritten, um Bitdefender Total Security 2018 auf Ihrem PC zu installieren.

# Schritt 1 - Installation von Bitdefender

Bevor Sie mit Installation fortfahren können, müssen Sie zunächst der Abonnementvereinbarung zustimmen. Bitte nehmen Sie sich einen Moment Zeit, um die Abonnementvereinbarung zu lesen, da Sie hier die Bedingungen finden, unter denen Sie Bitdefender Total Security 2018 nutzen dürfen.

Sollten Sie diesen Nutzungsbedingungen nicht zustimmen, schließen Sie das Fenster. Der Installationsprozess wird abgebrochen uns Sie verlassen den Assistenten.

In diesem Schritt können Sie zwei zusätzliche Dinge tun:

- Lassen Sie die Option **Anonyme Nutzungsstatistiken senden** aktiviert. Bleibt diese Option aktiviert, werden Berichte mit Informationen über Ihre Nutzung des Produkts an die Bitdefender-Server übertragen. Diese Information ist wichtig für die Verbesserung des Produktes. Wir möchten

Sie darauf hinweisen, dass diese Berichte keine vertraulichen Daten wie Ihren Namen oder Ihre IP-Adresse enthalten und dass diese Daten nicht für kommerzielle Zwecke verwendet werden.

- Wählen Sie die Sprache aus, in der das Produkt installiert werden soll.

Klicken Sie auf **INSTALLIEREN**, um den Installationsvorgang für Ihr Bitdefender-Produkt zu starten.

## Schritt 2 - Installation wird durchgeführt

Bitte warten Sie, bis der Installationsvorgang abgeschlossen ist. Sie erhalten detaillierte Informationen über den Fortschritt der Installation.

Kritische Bereiche Ihres Systems werden nach Bedrohungen durchsucht, die neuesten Versionen der Anwendungsdateien heruntergeladen und installiert und die Bitdefender-Dienste gestartet. Dieser Schritt kann einige Minuten in Anspruch nehmen. Klicken Sie auf **VOM SCAN AUSLASSEN**, wenn Sie Ihr System zu einem späteren Zeitpunkt scannen wollen. Weitere Informationen zur Durchführung eines System-Scans finden Sie im Kapitel *„Durchführen von System-Scans“* (S. 99).

## Schritt 3 - Installation ist abgeschlossen

Ihr Bitdefender-Produkt wurde erfolgreich installiert.

Eine Zusammenfassung der Installation wird angezeigt. Sollte während der Installation aktive Bedrohungen erkannt und entfernt werden, könnte ein Neustart des Systems erforderlich werden. Klicken Sie zum Fortfahren auf **Bitdefender** JETZT NUTZEN.

## Schritt 4 - Erste Schritte

Im Fenster **Erste Schritte** erhalten Sie erweiterte Informationen zu Ihrem aktivem Abonnement.

Klicken Sie auf **FERTIGSTELLEN**, um die Bitdefender Total Security 2018-Benutzeroberfläche aufzurufen.

## Installation vom Installationsdatenträger

Um Bitdefender vom Installationsdatenträger aus zu installieren, legen Sie den Datenträger in das optische Laufwerk ein.

Ein Installationsbildschirm sollte nach wenigen Augenblicken angezeigt werden. Folgen Sie den Anweisungen, um die Installation zu starten.

Wenn der Installationsbildschirm nicht angezeigt wird, öffnen Sie im Windows Explorer das Root-Verzeichnis des Datenträgers und doppelklicken Sie auf autorun.exe.

Bei langsamen Internetverbindungen oder falls Sie über keine Internetverbindungen verfügen, klicken Sie auf **Von CD/DVD installieren**. In diesem Fall wird das auf dem Datenträger befindliche Bitdefender-Produkt installiert. Eine neuere Version wird dann im Zuge des Produktupdates zu einem späteren Zeitpunkt von den Bitdefender-Servern heruntergeladen.

## Validierung der Installation

Bitdefender wird zuallererst Ihr System überprüfen, um die Installation zu bestätigen.

Wenn Ihr System die Mindestanforderungen zur Installation von Bitdefender nicht erfüllt, werden Sie darüber informiert, welche Bereiche aufgerüstet werden müssen, damit Sie fortfahren können.

Wenn eine inkompatible Sicherheitslösung oder eine ältere Version von Bitdefender erkannt wird, werden Sie aufgefordert, diese von Ihrem System zu entfernen. Bitte folgen Sie den Anweisungen, um die Software von Ihrem System zu entfernen und so spätere Probleme zu vermeiden. Unter Umständen müssen Sie Ihren Computer neu starten, um die Entfernung der erkannten Sicherheitslösungen abzuschließen.

### Beachten Sie

Das Herunterladen der Installationsdateien kann eine Weile dauern, besonders bei langsameren Internetverbindungen.

Sobald die Installation validiert ist, startet der Installationsassistent. Folgen Sie den Schritten, um Bitdefender Total Security 2018 auf Ihrem PC zu installieren.

## Schritt 1 - Installation von Bitdefender

Bevor Sie mit Installation fortfahren können, müssen Sie zunächst der Abonnementvereinbarung zustimmen. Bitte nehmen Sie sich einen Moment Zeit, um die Abonnementvereinbarung zu lesen, da Sie hier die Bedingungen finden, unter denen Sie Bitdefender Total Security 2018 nutzen dürfen.

Sollten Sie diesen Nutzungsbedingungen nicht zustimmen, schließen Sie das Fenster. Der Installationsprozess wird abgebrochen uns Sie verlassen den Assistenten.

In diesem Schritt können Sie zwei zusätzliche Dinge tun:

- Lassen Sie die Option **Anonyme Nutzungsstatistiken senden** aktiviert. Bleibt diese Option aktiviert, werden Berichte mit Informationen über Ihre Nutzung des Produkts an die Bitdefender-Server übertragen. Diese Information ist wichtig für die Verbesserung des Produktes. Wir möchten Sie darauf hinweisen, dass diese Berichte keine vertraulichen Daten wie Ihren Namen oder Ihre IP-Adresse enthalten und dass diese Daten nicht für kommerzielle Zwecke verwendet werden.
- Wählen Sie die Sprache aus, in der das Produkt installiert werden soll.

Klicken Sie auf **INSTALLIEREN**, um den Installationsvorgang für Ihr Bitdefender-Produkt zu starten.

## Schritt 2 - Installation wird durchgeführt

Bitte warten Sie, bis der Installationsvorgang abgeschlossen ist. Sie erhalten detaillierte Informationen über den Fortschritt der Installation.

Kritische Systembereiche werden auf Bedrohungen geprüft und die Bitdefender-Dienste gestartet. Dieser Schritt kann einige Minuten in Anspruch nehmen. Klicken Sie auf **VOM SCAN AUSLASSEN**, wenn Sie Ihr System zu einem späteren Zeitpunkt scannen wollen. Weitere Informationen zur Durchführung eines System-Scans finden Sie im Kapitel *„Durchführen von System-Scans“* (S. 99).

## Schritt 3 - Installation ist abgeschlossen

Eine Zusammenfassung der Installation wird angezeigt. Sollte während der Installation aktive Bedrohungen erkannt und entfernt werden, könnte ein Neustart des Systems erforderlich werden. Klicken Sie zum Fortfahren auf **Bitdefender** JETZT NUTZEN.

## Schritt 4 - Bitdefender-Konto

Nach Abschluss der ersten Einrichtung wird das Bitdefender-Konto Fenster angezeigt. Zur Aktivierung des Produktes und zur Nutzung seiner

Online-Funktionen wird ein Bitdefender-Benutzerkonto benötigt. Weitere Informationen finden Sie unter „*Bitdefender Central*“ (S. 38).

Fahren Sie entsprechend Ihrer Situation fort.

**Ich möchte ein Bitdefender-Konto anlegen**

Geben Sie die erforderlichen Informationen in die entsprechenden Felder ein und klicken Sie auf **BENUTZERKONTO ANLEGEN**.

Die hier eingetragenen Daten bleiben vertraulich.

Das Passwort muss mindestens 8 Zeichen lang sein und eine Zahl enthalten.

Lesen Sie die Bitdefender-Nutzungsbedingungen, bevor Sie fortfahren.

### Beachten Sie

Sobald das Benutzerkonto angelegt wurde, können Sie sich mit der angegebenen E-Mail-Adresse und dem Passwort unter https://central.bitdefender.com bei Ihrem Konto anmelden.

**Ich habe bereits ein Bitdefender Benutzerkonto.**

Klicken Sie auf **Anmelden** und geben Sie die E-Mail-Adresse und das Passwort für Ihr Bitdefender-Benutzerkonto ein.

Klicken Sie zum Fortfahren auf **ANMELDEN**.
Falls Sie das Passwort für Ihr Benutzerkonto vergessen haben oder Ihr bestehendes Passwort zurücksetzen möchten, klicken Sie auf **Mein Passwort vergessen**. Geben Sie Ihre E-Mail-Adresse ein und klicken Sie danach auf **PASSWORT VERGESSEN**. Rufen Sie Ihre E-Mails ab und folgen Sie der Anleitung, um ein neues Passwort für Ihr Bitdefender-Konto festzulegen.

### Beachten Sie

Falls Sie bereits über ein MyBitdefender-Benutzerkonto verfügen, können Sie sich mit den Zugangsdaten bei Bitdefender-Konto anmelden. Falls Sie Ihr Passwort vergessen haben, müssen Sie es unter https://my.bitdefender.com zunächst zurücksetzen. Verwenden Sie danach die aktualisierten Zugangsdaten, um sich bei Ihrem Bitdefender-Konto anzumelden.

**Ich möchte mich über mein Microsoft-, Facebook- oder Google-Konto anmelden**

So können Sie sich mit Ihrem Microsoft-, Facebook- oder Google-Konto anmelden:

1. Wählen Sie, worüber Sie sich anmelden möchten. Sie werden auf die Anmeldeseite dieses Dienstes weitergeleitet.
2. Folgen Sie den Anweisungen des ausgewählten Dienstes, um Ihr Benutzerkonto mit Bitdefender zu verknüpfen.

> **Beachten Sie**
> Bitdefender hat keinen Zugriff auf Ihre vertraulichen Informationen, so zum Beispiel das Passwort, das Sie zur Anmeldung in Ihrem Konto verwenden, oder die persönlichen Informationen Ihrer Freunde und Kontakte.

## Schritt 5 - Produkt aktivieren

> **Beachten Sie**
> Dieser Schritt muss durchgeführt werden, falls Sie sich im vorausgegangenem Schritt für die Anlage eines neuen Bitdefender-Konto entschieden haben oder sich mit einem Benutzerkonto angemeldet haben, für das das Abonnement bereits abgelaufen ist.

Zum Abschluss der Produktaktivierung wird eine aktive Internet-Verbindung benötigt.

Gehen Sie abhängig von Ihrer persönlichen Situation folgendermaßen vor:

- Ich habe einen Aktivierungscode

  In diesem Fall aktivieren Sie das Produkt, indem Sie die folgenden Schritte durchführen:

  1. Geben Sie den Aktivierungscode in das Feld **Ich habe einen Aktivierungscode** ein und klicken Sie auf **FORTFAHREN**.

     > **Beachten Sie**
     > Hier finden Sie Ihren Aktivierungscode:
     > - auf dem Label der CD/DVD.
     > - Auf der Registrierungskarte des Produktes.
     > - In der E-Mail-Bestätigung des Online-Kaufs.

2. **Ich möchte Bitdefender testen**

   In diesem Fall können Sie das Produkt für 30 Tage nutzen. Um Ihre Testphase zu starten, klicken Sie auf **Ich habe kein Abonnement, ich möchte das Produkt kostenlos testen** und danach auf **FORTFAHREN**.

## Schritt 6 - Erste Schritte

Im Fenster **Erste Schritte** erhalten Sie erweiterte Informationen zu Ihrem aktivem Abonnement.

Klicken Sie auf **FERTIGSTELLEN**, um die Bitdefender Total Security 2018-Benutzeroberfläche aufzurufen.

# 2. INBETRIEBNAHME

## 2.1. Grundlagen

Sobald Sie Bitdefender Total Security 2018 installiert haben, ist Ihr Computer gegen jede Art von Bedrohungen (wie beispielsweise Malware, Spyware, Ransomware, Exploits, Botnets und Trojaner) und andere Internetbedrohungen (wie Hacker, Phishing und Spam) geschützt.

Die Anwendung nutzt die Photon-Technologie, um Bedrohungs-Scans zu beschleunigen und noch leistungsfähiger zu machen. Diese lernt, wie Sie die Anwendungen auf Ihrem System nutzen, und weiß so, was sie wann scannen soll. Dadurch werden die Auswirkungen auf die Systemleistung minimiert.

Ungeschützte Verbindungen mit öffentlichen WLAN-Netzwerken in Flughäfen, Einkaufszentrum, Cafés oder Hotels geht mir Risiken für Ihr Gerät und Ihre Daten verbunden. Nicht nur weil Betrüger Ihre Aktivitäten vielleicht überwachen, um einen günstigen Moment für den Diebstahl Ihrer persönlichen Daten abzupassen, sondern auch weil Ihre IP-Adresse für jedermann sichtbar ist, was Ihren Computer anfällig für zukünftige Cyberangriffe macht. Vermeiden Sie derartige unglückliche Situationen, indem Sie die *„VPN“* (S. 161)-App installieren.

Behalten Sie den Überblick über Ihre Passwörter und Online-Konten, indem Sie sie *„Passwortmanager-Schutz für Ihre Anmeldedaten“* (S. 154) in einer Geldbörse sicher verwahren. Mit nur einem Masterpasswort können Sie Ihre Privatsphäre vor Eindringlingen schützen, die es auf Ihr Geld abgesehen haben.

*„Webcam-Schutz“* (S. 142)verhindert, dass nicht vertrauenswürdige Apps auf Ihre Kamera zugreifen und unterbindet so Hacking-Versuche. Der Bitdefender-Benutzer entscheidet, welche Apps auf Ihre Webcam zugreifen dürfen und welche blockiert werden.

Um Sie vor Datenjägern und -schnüfflern in nicht gesicherten Drahtlosnetzwerken zu schützen, prüft Bitdefender zunächst die Sicherheit des Netzwerks und gibt falls erforderlich Empfehlungen, um Ihre Online-Sicherheit zu steigern. Eine Anleitung zum Schutz Ihrer privaten Daten finden Sie im Kapitel *„WLAN-Sicherheitsberater“* (S. 139).

So liegen Ihre persönlichen Dateien, so zum Beispiel lokal oder in der Cloud gespeicherte Dokumente, Fotos und Videos, außerhalb der Reichweite der

wohl gefährlichsten Bedrohung unserer Zeit: Ransomware. Weitere Informationen zum Schutz Ihrer persönlichen Dateien finden Sie im Kapitel *„Sichere Dateien“ (S. 145)*.

Bitdefender ermöglicht Ihnen ein störungsfreies Arbeiten, Spielen und Abspielen von Filmen, indem es Wartungsaufgaben aufschiebt, Unterbrechungen verhindert und die visuellen Einstellungen entsprechend anpasst. Sie können von all dem profitieren, indem Sie Ihre *„Profile“ (S. 192)*.

Bitdefender trifft alle sicherheitsrelevanten Entscheidungen für Sie und wird nur in seltenen Fällen Pop-up-Benachrichtigungen anzeigen. Nähere Informationen zu den durchgeführten Aktionen und zur Programmausführung finden Sie im Fenster Benachrichtigungen. Weitere Informationen finden Sie unter *„Nachrichten“ (S. 16)*.

Von Zeit zu Zeit sollten Sie Bitdefender öffnen und existierende Probleme beheben. Es ist möglich, dass Sie, um Ihren Computer und Ihre Daten zu schützen, bestimmte Bitdefender-Komponenten konfigurieren oder vorbeugende Maßnahmen durchführen müssen.

Rufen Sie Ihr Bitdefender-Benutzerkonto auf, um die Online-Funktionen von Bitdefender Total Security 2018 zu nutzen und Ihre Abonnements und Geräte zu verwalten. Weitere Informationen finden Sie unter *„Bitdefender Central“ (S. 38)*.

Im Abschnitt *„Gewusst wie“ (S. 51)* finden Sie detaillierte Anweisungen zur Ausführung der häufigsten Aufgaben. Wenn Sie bei der Verwendung von Bitdefender Probleme haben, finden Sie im Abschnitt *„Verbreitete Probleme beheben“ (S. 200)* Lösungen zu den häufigsten Problemen.

## Das Bitdefender-Fenster öffnen

Um das Bitdefender Total Security 2018-Hauptfenster aufzurufen, gehen Sie folgendermaßen vor:

- In **Windows 7**:
  1. Klicken Sie auf **Start** und **Alle Programme**.
  2. Klicken Sie auf **Bitdefender 2018**.
  3. Klicken Sie auf **Bitdefender Total Security 2018**. Noch schneller geht es mit einem Doppelklick auf das Bitdefender-Symbol in der Task-Leiste.
- In **Windows 8 und Windows 8.1**:

Finden Sie auf der Windows-Startseite Bitdefender (z.B. durch die Eingabe von "Bitdefender" auf der Startseite) und klicken Sie auf das entsprechende Symbol. Öffnen Sie alternativ die Desktop-App und doppelklicken Sie danach auf das Bitdefender-Symbol in der Task-Leiste.

- In **Windows 10**:

  Geben Sie im Suchfeld in der Taskleiste "Bitdefender" ein und klicken Sie auf das entsprechende Symbol. Alternativ ist auch ein Doppelklick auf das Bitdefender -Symbol in der Taskleiste möglich.

Weitere Informationen zum Bitdefender-Fenster und zum Symbol in der Task-Leiste finden Sie im Kapitel *„Bitdefender-Benutzeroberfläche“* (S. 21).

### 2.1.1. Probleme beheben

Bitdefender benutzt ein Problem-Tracking-System, um sicherheitsgefährdende Probleme festzustellen und Sie über diese zu informieren. Standardmässig wird nur ein Teil der für am wichtigsten erachteten Risiken überwacht. Sie können dies nach Bedarf verändern, wählen Sie aus über welche Risiken sie informiert werden möchten.

Zu den gefundenen Problemen gehören auch wichtige Schutzeinstellungen, die deaktiviert sind, und andere Umstände, die ein Sicherheitsrisiko darstellen. Sie sind in zwei Kategorien unterteilt:

- **Kritische Probleme** - Verhindern, dass Bitdefender Sie vor Bedrohungen schützt oder stellen ein erhebliches Sicherheitsrisiko dar.
- **Kleinere (nicht-kritische) Probleme** - Können Ihren Schutz in naher Zukunft beeinträchtigen.

Das Bitdefender-Symbol in der Task-Leiste weist Sie durch die folgenden Farbwechsel auf ausstehende Probleme hin:

Die Sicherheit Ihres Systems wird durch kritische Probleme beeinträchtigt. Sie benötigen Ihre sofortige Aufmerksamkeit und müssen umgehend behoben werden.
Die Sicherheit Ihres Systems wird durch nicht-kritische Probleme beeinträchtigt. Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben.

Wenn Sie den Mauszeiger über das Symbol bewegen, wird Ihnen angezeigt, dass ein Problem existiert.

Nach dem Öffnen der Bitdefender-Benutzeroberfläche zeigt der Sicherheitsstatusbereich in der oberen Symbolleiste die Art der Probleme an, die Ihr System beeinträchtigen.

## Assistent für Sicherheitsprobleme

Um erkannte Probleme zu beheben, folgen Sie den Anweisungen des **Sicherheitsprobleme**-Assistenten.

1. Befolgen Sie eine der folgenden Möglichkeiten, den Assistenten zu öffnen:
   - Rechtsklicken Sie auf das Bitdefender-Symbol in der Task-Leiste und wählen Sie dann **Sicherheitsprobleme anzeigen**.
   - Öffnen Sie die Bitdefender-Benutzeroberfläche und klicken Sie auf eine beliebige Stelle innerhalb des Sicherheitsstatusbereichs in der oberen Symbolleiste.
2. Sie erhalten eine Übersicht aller Probleme, die die Sicherheit Ihres Computers und Ihrer Daten beeinträchtigen. Alle aktuellen Probleme sind markiert und werden behoben.

   Wenn Sie ein bestimmtes Problem nicht sofort beheben möchten, deaktivieren Sie das entsprechende Kästchen. Sie werden aufgefordert anzugeben, für wie lange die Behebung des Problems verschoben werden soll. Wählen Sie die gewünschte Option aus dem Menü und klicken Sie auf **OK**. Um die Überwachung der jeweiligen Problemkategorie zu beenden, wählen Sie den Punkt **Dauerhaft**.

   Der Status des Problems erscheint als **Aufgeschoben** und es wird keine Aktion zur Behebung des Problems durchgeführt.
3. Um die ausgewählten Probleme zu beheben, klicken Sie auf **Beheben**. Manche Probleme werden sofort behoben. Bei anderen hilft Ihnen ein Assistent bei der Behebung.

Die Risiken die Ihnen dieser Assistent hilft zu beheben, können in diese Hauptkategorien eingeordnet werden

- **Deaktivierte Sicherheitseinstellungen.** Solche Probleme werden sofort beseitigt, durch die entsprechenden Sicherheitseinstellungen.
- **Vorbeugende Sicherheitsaufgaben die Sie durchführen sollten.** Bei der Beseitigung solcher Probleme, hilft Ihnen ein Assistent.

## Konfigurieren von Statusbenachrichtigungen

Bitdefender kann Sie informieren, wenn in einer der folgenden Komponenten ein Problem aufgetreten ist:

- Virenschutz
- Firewall
- Update (Aktualisierung)
- Browser-Sicherheit

Sie können das Warnsystem ganz nach Ihren individuellen Ansprüchen konfigurieren, indem Sie wählen, über welche Ereignisse Sie informiert werden möchten. Folgen Sie diesen Schritten:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **ERWEITERT**.
3. Klicken Sie auf **Statusbenachrichtigungen konfigurieren**.
4. Klicken Sie auf die Schalter, um die Statusbenachrichtigungen entsprechend Ihrer Anforderungen zu aktivieren oder zu deaktivieren.

## 2.1.2. Nachrichten

Bitdefender führt ein detailliertes Ereignisprotokoll über alle Aktivitäten der Software auf Ihrem Computer. Immer wenn etwas passiert, was die Sicherheit Ihres Systems oder Ihrer Daten betrifft, wird in den Bitdefender-Benachrichtigungen eine Nachricht erstellt, ähnlich einer neuen E-Mail in Ihrem Postfach.

Benachrichtigungen sind ein wichtiges Hilfsmittel für die Überwachung und Verwaltung Ihres Bitdefender-Schutzes. So können Sie z. B. überprüfen, ob ein Update erfolgreich durchgeführt wurde oder ob Bedrohungen oder Schwachstellen im System gefunden wurden. Zudem können Sie bei Bedarf weitere Aktionen ausführen oder die von Bitdefender ausgeführten Aktionen anpassen.

Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol, um auf das Benachrichtigungsprotokoll zuzugreifen. Bei jedem kritischen Ereignis wird auf dem -Symbol ein Zähler eingeblendet.

Je nach Art und Schwere werden Benachrichtigungen sortiert nach:

- **Kritische** Ereignisse weisen auf kritische Probleme hin. Sie sollten sich umgehend darum kümmern.
- **Warnung** Diese Ereignisse weisen auf nicht-kritische Probleme hin. Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben.
- **Information** Diese Ereignisse weisen auf erfolgreich ausgeführte Vorgänge hin.

Mit einem Klick auf den jeweiligen Reiter erhalten Sie weitere Informationen zu den Ereignissen. Mit einem einfachen Klick auf den Ereignisnamen werden die folgenden Kurzinfos angezeigt: Kurzbeschreibung, die von Bitdefender durchgeführte Aktion sowie Datum und Zeitpunkt des Ereignisses. Unter Umständen werden Ihnen Optionen zur weiteren Vorgehensweise angeboten.

Zur übersichtlicheren Verwaltung der protokollierten Ereignisse enthält das Benachrichtigungsfenster Optionen, mit denen Sie alle Ereignisse in einem Abschnitt löschen oder als gelesen markieren können.

### 2.1.3. Autopilot

Für alle Benutzer, die nichts weiter von Ihrer Sicherheitslösung erwarten, als zuverlässigen Schutz, ohne bei der Arbeit gestört zu werden, bietet Bitdefender Total Security 2018 einen integrierten Autopilot-Modus.

Solange der Autopilot aktiviert ist, wird Bitdefender die optimale Sicherheitskonfiguration anwenden und alle sicherheitsrelevanten Entscheidungen für Sie treffen. Das bedeutet, dass nur äußerst selten Pop-ups eingeblendet werden und Sie keinerlei Einstellungen vornehmen müssen.

Wenn der AutoPilot aktiviert ist, werden kritische Probleme von Bitdefender automatisch behoben. Zudem werden die folgenden Funktionen unauffällig im Hintergrund verwaltet:

- Virenschutz, gewährleistet durch Zugriff-Scans und ununterbrochenes Scanning.
- Firewall-Schutz.
- Internet-Schutz.
- Automatische Updates.

Sie können den Autopilot mit einem Klick auf den **AUTOPILOT**-Schalter in der oberen Symbolleiste der Bitdefender-Benutzeroberfläche aktivieren oder deaktivieren.

Wenn der Autopilot eingeschaltet ist, erscheint folgendes Bitdefender-Symbol in der Task-Leiste: .

**Wichtig**
Wenn der Autopilot eingeschaltet ist und Sie eine der von ihm verwalteten Einstellungen verändern, wird er automatisch ausgeschaltet.

Um eine Übersicht der Aktionen anzuzeigen, die von Bitdefender durchgeführt wurden, während der Autopilot eingeschaltet war, öffnen Sie das Fenster Benachrichtigungen.

## 2.1.4. Profile

Bei einigen Aktivitäten am Computer, so zum Beispiel bei Online-Spielen oder Videopräsentationen, werden schnelle Reaktionszeiten und konstant hohe Systemleistung ohne Unterbrechungen benötigt. Wenn Ihr Laptop auf Batteriebetrieb läuft ist es ratsamer unnötige Vorgänge, welche zusätzlich Strom verbrauchen, zu verschieben, bis der Laptop extern mit Strom versorgt wird.

Bitdefender-Profile weist den laufenden Anwendungen zusätzliche Systemressourcen zu, indem er die Schutzeinstellungen vorübergehend modifiziert und die Systemkonfiguration entsprechend anpasst. So werden die Systemauswirkungen auf Ihre jeweilige Aktivität minimiert.

Um den verschiedenen Aktivitäten gerecht zu werden, enthält Bitdefender die folgenden Profile:

Arbeitsprofil
: Sorgt für optimale Arbeitseffizienz, indem es die Produkt- und Systemeinstellungen erkennt und entsprechend anpasst.

Filmprofil
: Verbessert die visuellen Effekte und sorgt für störungsfreies Filmvergnügen.

Spielprofil
: Verbessert die visuellen Effekte und sorgt für störungsfreies Spielvergnügen.

Öffentliches WLAN-Profil
: Wendet Produkteinstellungen an, um Ihnen auch bei Verbindungen mit unsicheren WLAN-Netzwerken umfassenden Schutz zu bieten.

Akkubetriebsprofil
: Wendet Produkteinstellungen an und stoppt Hintergrundaktivitäten, um die Akkulaufzeit zu verlängern.

## Automatische Aktivierung von Profilen konfigurieren

Für noch mehr Benutzerfreundlichkeit können Sie Bitdefender so konfigurieren, dass es Ihr Arbeitsprofil verwaltet. In diesem Fall erkennt Bitdefender automatisch Ihre jeweiligen Aktivitäten und optimiert den System- und Produktbetrieb entsprechend.

So erlauben Sie Bitdefender die Aktivierung von Profilen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das ⚙-Symbol.
2. Wechseln Sie zum Reiter **PROFILE**.
3. Über den entsprechenden Schalter können Sie die Option **Profile automatisch aktivieren** einschalten.

Wenn Sie nicht möchten, dass die Profile automatisch aktiviert werden, deaktivieren Sie den Schalter.

Klicken Sie zur manuellen Aktivierung eines Profils auf den entsprechenden EIN/AUS-Schalter. Es kann je nur ein Profil gleichzeitig manuell aktiviert werden.

Weitere Informationen zu den Profilen finden Sie im Kapitel„*Profile*“ (S. 192)

## 2.1.5. Passwortschutz für Bitdefender-Einstellungen

Wenn Sie nicht der einzige Benutzer des Computers sind, empfehlen wir Ihnen, Ihre vorgenommenen Einstellungen mit einem Passwort zu schützen.

So können Sie den Passwortschutz für die Bitdefender-Einstellungen konfigurieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das ⚙-Symbol.
2. Aktivieren Sie im Fenster **ALLGEMEIN** den **PASSWORTSCHUTZ**, indem Sie auf den entsprechenden Schalter klicken.
3. Geben Sie das Passwort in beide Felder ein und klicken Sie dann auf **OK**. Das Passwort muss mindestens 8 Zeichen lang sein.

Sobald Sie ein Passwort festgelegt haben, muss jeder, der die Bitdefender-Einstellungen verändern will, zunächst das Passwort eingeben.

**Wichtig**

Merken Sie sich Ihr Passwort gut oder schreiben Sie es auf und verwahren es an einem sicheren Platz. Wenn Sie Ihr Passwort vergessen haben, müssen Sie das Programm neu installieren oder den Kundendienst von Bitdefender kontaktieren.

So können Sie den Passwortschutz aufheben:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das ⚙-Symbol.
2. Deaktivieren Sie im Fenster **ALLGEMEIN** den Passwortschutz, indem Sie auf den entsprechenden Schalter klicken.
3. Geben Sie das Passwort ein und klicken Sie auf **OK**.

**Beachten Sie**

Um das Passwort für Ihr Produkt zu ändern, klicken Sie auf **Passwort ändern**. Geben Sie Ihr aktuelles Passwort ein und klicken Sie auf *OK*. Geben Sie im Fenster, das jetzt angezeigt wird, das neue Passwort ein, mit dem Sie ab jetzt den Zugang zu Ihren Bitdefender-Einstellungen einschränken wollen.

## 2.1.6. Anonyme Nutzungsberichte

Bitdefender verschickt standardmäßig Berichte mit Nutzungsinformationen an die Bitdefender-Server. Diese Information ist wichtig für die Verbesserung des Produktes. Wir möchten Sie darauf hinweisen, dass diese Berichte keine vertraulichen Daten wie Ihren Namen oder Ihre IP-Adresse enthalten und dass diese Daten nicht für kommerzielle Zwecke verwendet werden.

So können Sie den Versand von anonymen Nutzungsberichten einstellen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das ⚙-Symbol.
2. Wechseln Sie zum Reiter **ERWEITERT**.
3. Klicken Sie auf die entsprechenden EIN/AUS-Schalter.

### 2.1.7. Benachrichtigungen zu Sonderangeboten

Sind Sonderangebote verfügbar, wird das Bitdefender-Produkt Sie per Pop-up-Benachrichtigung darüber informieren. So können Sie von unseren Vorteilspreisen profitieren und Ihre Geräte länger schützen.

So können Sie Benachrichtigungen über Sonderangebote aktivieren oder deaktivieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das ⚙-Symbol.
2. Klicken Sie Fenster **ALLGEMEIN** auf den entsprechenden EIN/AUS-Schalter.

Die Option für die Benachrichtigungen zu Sonderangeboten und dem Produkt ist standardmäßig aktiviert.

## 2.2. Bitdefender-Benutzeroberfläche

Bitdefender Total Security 2018 entspricht den Bedürfnissen sowohl von Profis als auch von Beginnern. Die grafische Benutzeroberfläche ist so konzipiert, dass Sie für jeden Benutzer anpassbar ist.

Oben links wird ein Assistent eingeblendet, der Sie durch die Elemente der Bitdefender-Oberfläche leitet und Ihnen bei der Konfiguration zur Seite steht. Wählen Sie **WEITER**, um dem Assistenten weiter zu folgen, oder **Einführung überspringen**, um den Assistenten zu schließen.

Um den Produktstatus abzurufen und grundlegende Aufgaben auszuführen, steht Ihnen das Bitdefender-Symbol in der Task-Leiste jederzeit zur Verfügung.

Über das Hauptfenster können Sie mithilfe des Autopiloten das Produktverhalten steuern, auf wichtige Produktinformationen zugreifen und die häufigsten Aufgaben starten. Über den Bereich links können Sie auf Bitdefender-Konto und die Bitdefender-Bereiche zugreifen, um detaillierte Konfigurationen vorzunehmen und erweiterte administrative Aufgaben zu starten.

Wenn Sie wichtige Sicherheitsinformationen ständig im Blick haben und direkten Zugriff auf wichtige Einstellungen haben möchten, können Sie das Sicherheits-Widget zu Ihrem Desktop hinzufügen.

## 2.2.1. Task-Leisten-Symbol

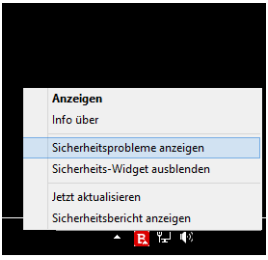
Um das gesamte Produkt schneller zu verwalten, können Sie das Bitdefender-Symbol in der Task-Leiste nutzen.

### Beachten Sie

Das Bitdefender-Symbol ist unter Umständen nicht immer sichtbar. So können Sie das Symbol dauerhaft anzeigen lassen:

- In **Windows 7, Windows 8 und Windows 8.1**:
  1. Klicken Sie auf den Pfeil in der unteren rechten Ecke des Bildschirms.
  2. Klicken Sie auf **Benutzerdefiniert ...**, um das Fenster der Infobereichsymbole zu öffnen.
  3. Wählen Sie **Symbole und Benachrichtigungen anzeigen** für das Symbol **Bitdefender Agent**.
- In **Windows 10**:
  1. Rechtsklicken Sie auf der Leiste und wählen Sie **Eigenschaften**.
  2. Klicken Sie im Fenster der Taskleiste auf **Anpassen**.
  3. Klicken Sie im Fenster **Benachrichtigungen & Aktionen** auf den Link **Klicken Sie hier, um die Symbole auszuwählen, die auf der Taskleiste angezeigt werden.**.
  4. Aktivieren Sie den Schalter neben **Bitdefender-Agent**.

Wenn Sie dieses Icon doppelklicken wird sich Bitdefender öffnen. Wird das Symbol mit der rechten Maustaste angeklickt, öffnet sich ein Kontextmenü, mit dem Sie das BitdefenderProdukt verwalten können.



Tray Icon

- **Anzeigen** - Öffnet das Bitdefender-Hauptfenster.
- **Über** - Öffnet ein Fenster mit Informationen zu Bitdefender. Sie erfahren zudem, wo Sie bei unerwarteten Problemen Hilfe finden können und wo Sie die Abonnementvereinbarung sowie Informationen zu Komponenten von Drittanbietern und die Datenschutzrichtlinie nachlesen können.
- **Sicherheitsprobleme anzeigen** - hilft bestehende Sicherheitsschwachstellen zu entfernen. Falls

die Option nicht verfügbar ist, so gibt es keine zu behebenden Probleme. Detaillierte Informationen finden Sie unter *„Probleme beheben“ (S. 14)*.

- **Sicherheits-Widget anzeigen/ausblenden** - aktiviert/deaktiviert das Sicherheits-Widget.
- **Jetzt Aktualisieren** - startet ein sofortiges Update. Sie können den Update-Status im Update-Bereich des Bitdefender Hauptfensters verfolgen.
- **Sicherheitsbericht anzeigen** - Öffnet ein Fenster, in dem ein wöchentlicher Statusbericht sowie Empfehlungen für Ihr System angezeigt werden. Beachten Sie die Empfehlungen, um die Sicherheit Ihres Systems zu verbessern.

Das Bitdefender-Symbol in der System Tray informiert Sie über spezielle Symbole, über mögliche Probleme:

Kritische Probleme beeinträchtigen die Sicherheit Ihres Systems. Sie benötigen Ihre sofortige Aufmerksamkeit und müssen umgehend behoben werden.
Die Sicherheit Ihres Systems wird durch nicht-kritische Probleme beeinträchtigt. Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben.
Der Bitdefender-Autopilot ist aktiviert.

Wenn Bitdefender nicht aktiv ist, ist das Symbol in der Task-Leiste grau hinterlegt: . Dies geschieht normalerweise, wenn das Abonnement abgelaufen ist. Es kann auch vorkommen, wenn die Bitdefender Services nicht reagieren oder andere Fehler die normale Funktionsweise von Bitdefender einschränken.

## 2.2.2. Hauptfenster

Im Bitdefender-Hauptfenster können Sie die häufigsten Aufgaben durchführen, Sicherheitsprobleme schnell und einfach beheben, Informationen über die Programmausführung anzeigen und auf die verschiedenen Bereiche zugreifen, über die sich die Produkteinstellungen konfigurieren lassen. Und das alles mit nur wenigen Klicks.

Das Fenster ist in 4 Hauptbereiche aufgeteilt:

Statusbereich
: Hier können Sie den Sicherheitsstatus Ihres Computers einsehen, Updates starten und den Autopilot konfigurieren.

Linker Seitenbereich
: Über dieses Menü können Sie Bitdefender-Konto und die Online-Funktionen Ihres Produktes verwalten oder zwischen den drei Hauptbereichen des Produkt hin- und herschalten. Von hier aus können Sie zudem auf die Benachrichtigungen, den wöchentlichen Sicherheitsbericht, die allgemeinen Einstellungen und die Support-Bereiche zugreifen.

Schaltflächen und Zugriff auf die Funktionen
: Hier können Sie verschiedene Aufgaben ausführen, um Ihr System zu schützen und Systemressourcen optimal zu nutzen. Darüber hinaus können Sie auf die Bitdefender-Funktionen zugreifen, um Ihr Produkt selbst zu konfigurieren.

Fußleiste
: Hier können Sie unkompliziert Bitdefender auf anderen Geräten installieren, sofern Ihr Abonnement genügend freie Arbeitsplätze hat.

## Statusbereich

Der Statusbereich enthält die folgenden Elemente:

- Der **Sicherheitsstatus** links informiert Sie darüber, ob Probleme die Sicherheit Ihres Computers beeinträchtigen und hilft Ihnen, diese zu beheben.

  Die Farbe des Sicherheitsstatusbereichs verändert sich abhängig von den erkannten Problemen. Zudem werden unterschiedliche Meldungen angezeigt:

  - **Der Bereich ist grün markiert.** Es müssen keine Probleme behoben werden. Ihr Rechner und Ihre Daten sind geschützt.
  - **Der Bereich ist gelb markiert.** Die Sicherheit Ihres Systems wird durch nicht-kritische Probleme beeinträchtigt. Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben.
  - **Der Bereich ist rot markiert.** Die Sicherheit Ihres Systems wird durch kritische Probleme beeinträchtigt. Sie sollten sich umgehend um diese Probleme kümmern.

  Mit einem Klick auf eine beliebige Stelle im Sicherheitsstatusbereich können Sie einen Assistenten aufrufen, mit dem Sie alle Bedrohungen einfach und schnell von Ihrem Computer entfernen können. Detaillierte Informationen finden Sie unter „*Probleme beheben*“ (S. 14).

- Mit dem **AUTOPILOT** sorgen Sie für optimalen Schutz und können den unauffälligen Hintergrundschutz für sich arbeiten lassen. Weitere Einzelheiten finden Sie im Kapitel *„Autopilot“* (S. 17).
- Über **JETZT AKTUALISIEREN** können Sie jederzeit ein Update durchführen, um sicherzustellen, dass Ihre Datenbank mit den Bedrohungsinformationen auf dem neuesten Stand ist. Weitere Einzelheiten finden Sie im Kapitel *„Bitdefender auf dem neuesten Stand halten“* (S. 46).
- Unter **Aktives Profil** sehen Sie das derzeit in Ihrem Bitdefender-Produkt aktivierte Profil. Weitere Einzelheiten finden Sie im Kapitel *„Profile“* (S. 192).

## Linker Seitenbereich

Im linken Seitenbereich finden Sie aussagekräftige Symbole, über die auf Bitdefender-Konto, die Produktbereiche, Aktivitätsberichte, Benachrichtigungen, allgemeine Einstellungen und den Supportbereich zugreifen können.

Die Name der Symbole werden mit einem Klick auf ≡ sichtbar:

- **Schutz**. Die Schaltflächen für den **Quick Scan** und den **Schwachstellen-Scan** werden unten links in der Bitdefender-Benutzeroberfläche eingeblendet. Darüber hinaus werden Informationen über blockierte Anwendungen, gefundene Bedrohungen und Angriffe eingeblendet. Klicken Sie auf den Link **FUNKTIONEN ANZEIGEN**, um den Konfigurationsbereich aufzurufen.
- **Benachrichtigungen**. Die Schaltflächen für **Safepay** und den **VPN** werden unten links in der Bitdefender-Benutzeroberfläche eingeblendet. Darüber hinaus werden Informationen über gefundene Geldbörsen und Datentresore eingeblendet. Klicken Sie auf den Link **FUNKTIONEN ANZEIGEN**, um den Konfigurationsbereich aufzurufen.
- **Extras**. Die Schaltflächen für die **Ein-Klick-Optimierung** und die **Systemstartoptimierung** werden unten links in der Bitdefender-Benutzeroberfläche eingeblendet. Darüber hinaus können Sie die Diebstahlschutzfunktion aufrufen und die **Disk Cleanup**-Funktion starten, um nicht mehr benötigte Dateien zu löschen und Speicherplatz freizugeben.

- **Aktivität**. Von hier aus können Sie die Produktaktivitäten der vergangenen 30 Tage einsehen und den wöchentlich generierten Sicherheitsbericht aufrufen.
- **Benachrichtigungen**. Von hier aus können Sie auf Ihre Benachrichtigungen zugreifen.
- **Konto**. Details zu Bitdefender-Konto und das aktuelle Abonnement sind verfügbar. In Ihrem Bitdefender-Konto können Sie Ihre Abonnements einsehen und auf den von Ihnen verwalteten Geräten Sicherheitsaufgaben ausführen.
- **Einstellungen**. Von hier aus können Sie auf die allgemeinen Einstellungen zugreifen.
- **Support**. Von hier aus können Sie jederzeit den technischen Support von Bitdefender kontaktieren, falls Sie Unterstützung mit Ihrem Bitdefender Total Security 2018 benötigen.

## Schaltflächen und Zugriff auf die Funktionen

Über die Schaltflächen können Sie schnell wichtige Aufgaben starten. Schaltflächen werden unten links in der Bitdefender-Benutzeroberfläche eingeblendet, wenn Sie einen der folgenden drei Bereiche im Seitenbereich links auswählen: **Schutz**, **Privatsphäre** oder **Extras**.

Je nach ausgewähltem Bereich werden die folgenden Schaltflächen im jeweiligen Bereich eingeblendet:

- **Quick-Scan**. Führen Sie einen Quick Scan durch, um sicherzustellen, dass Ihr Computer frei von Bedrohungen ist.
- **Schwachstellen-Scan**. Überprüfen Sie Ihren Computer nach Schwachstellen, um sicherzustellen, dass alle installierten Anwendungen und Ihr Betriebssystem auf dem neuesten Stand sind und ordnungsgemäß laufen.
- **Safepay**. Öffnen Sie Bitdefender Safepay™, um Ihre sensiblen Daten bei Online-Transaktionen zu schützen.
- **VPN**. Öffnen Sie Bitdefender VPN, um Ihre Internetverbindungen zusätzlich abzusichern.
- **Ein-Klick-Optimierung**. Gewinnen Sie Speicherplatz auf der Festplatte, beheben Sie Registry-Fehler und schützen Sie Ihre Privatsphäre, indem Sie nicht mehr benötigte Dateien mit nur einem Klick löschen.

- **Systemstart-optimierung**. Sorgen Sie für schnellere Systemstartzeiten, indem Sie nicht benötigte Anwendung aus dem Systemstart entfernen.

### Fußleiste

So schützen Sie weitere Geräte:

1. Klicken Sie auf den Link **AUF EINEM ANDEREN GERÄT INSTALLIEREN**.

   Sie werden auf die Bitdefender-Konto Website weitergeleitet. Stellen Sie sicher, dass Sie sich mit Ihren Anmeldedaten angemeldet haben.

2. Wählen Sie im angezeigten Fenster das gewünschte Betriebssystem und klicken Sie dann auf **FORTFAHREN**.

3. Geben Sie die E-Mail-Adresse ein, an die wir den Download-Link für die Installation auf der gewählten Plattform senden sollen.

Je nach Ihrer Wahl werden die folgenden Bitdefender-Produkte installiert:

- Bitdefender Total Security 2018 auf Windows-Geräten.
- Bitdefender Antivirus for Mac auf macOS-Geräten.
- Bitdefender Mobile Security auf Android-basierten Geräten.
- Bitdefender Mobile Security auf iOS-Geräten.
- Bitdefender-Elternberater auf macOS-, iOS- und Android-Geräten.

## 2.2.3. Die Bitdefender-Bereiche

Das Bitdefender-Produkt besteht aus drei in nützliche Funktionen unterteilten Bereichen, die Sie bei der Arbeit, beim Surfen im Internet und bei der Abwicklung von Online-Zahlungen schützen, Ihre Systemgeschwindigkeit deutlich steigern und viele weitere Vorteile bieten.

Um auf die Funktionen und bestimmte Bereiche zuzugreifen oder um Ihr Produkt zu konfigurieren, stehen in die folgenden Symbole im linken Seitenbereich der Bitdefender-Benutzeroberfläche zur Verfügung:

- Schutz
- Privatsphäre
- Extras

## Schutz

Im Bereich Schutz können Sie erweiterte Sicherheitseinstellungen vornehmen, Freunde und Spammer verwalten, die Netzwerkverbindungseinstellungen anzeigen und bearbeiten, die Funktionen für Sichere Dateien und Internet-Schutz konfigurieren, nach möglichem Sicherheitslücken im System suchen und diese beheben sowie die Sicherheit genutzter Drahtlosnetzwerke prüfen.

Im Bereich Schutz können Sie die folgenden Funktionen verwalten:

**ANTIVIRUS**

Der Virenschutz bildet die Grundlage Ihrer Sicherheit. Bitdefender schützt Sie sowohl in Echtzeit als auch bei Bedarf vor allen Arten von Bedrohungen, so zum Beispiel vor Malware, Trojanern, Spyware, Adware usw.

Über die Funktion Virenschutz können Sie schnell und bequem auf die folgenden Scan-Aufgaben zugreifen:

- Quick-Scan
- System-Scan
- Scans verwalten
- Rettungsmodus (Rettungsumgebung unter Windows 10)

Weitere Informationen zu den Scan-Aufgaben und eine Anleitung, wie Sie den Virenschutz konfigurieren können, finden Sie im Kapitel „*Virenschutz*“ (S. 91).

**INTERNET-SCHUTZ**

Mit dem Internet-Schutz schützen Sie sich beim Surfen zuverlässig vor Phishing-Angriffen, Betrugsversuchen und der unbeabsichtigten Weitergabe privater Daten.

Weitere Informationen, wie man Bitdefender zum Schutz Ihrer Internet-Aktivitäten konfigurieren kann, finden Sie im Kapitel „*Internet-Schutz*“ (S. 116).

**FIREWALL**

Die Firewall schützt Sie, während Sie mit Netzwerken und dem Internet verbunden sind, indem alle Verbindungsversuche gefiltert werden.

Weitere Informationen zur Firewall-Konfiguration finden Sie im Kapitel „*Firewall*“ (S. 128).

**ADVANCED THREAT DEFENSE**

Die Erweiterte Gefahrenabwehr schützt Ihr System aktiv vor Bedrohungen wie Ransomware, Spyware und Trojanern, indem es das Verhalten aller installierten Anwendungen untersucht. Verdächtige Prozesse werden erkannt und, falls erforderlich, blockiert.

Weitere Informationen zum Schutz Ihres Systems vor Bedrohungen finden Sie im Kapitel *„Advanced Threat Defense“* (S. 114).

**SPAM-SCHUTZ**

Das Spam-Schutz-Funktion von Bitdefender stellt sicher, dass Ihr Posteingang von unerwünschten E-Mails frei bleibt, indem es den POP3-Nachrichtenverkehr filtert.

Weitere Informationen zum Spam-Schutz finden Sie im Kapitel *„Spam-Schutz“* (S. 119).

**SCHWACHSTELLE**

Mit der Schwachstellenfunktionen können Sie Ihr Betriebssystem und Ihre am häufigsten verwendeten Anwendungen auf dem neuesten Stand halten und ungesicherte Drahtlosnetzwerke aufspüren.

Klicken Sie unter Schwachstellen auf **Schwachstellen-Scan**, um kritische Windows-Updates, Anwendungsupdates, schwache Passwörter für Windows-Konten und unsichere WLAN-Netzwerke zu finden.

Klicken Sie auf **WLAN-Sicherheitsberater**, um eine Liste Ihrer Drahtlosnetzwerke anzuzeigen. Sie erhalten eine Bewertung ihrer Sicherheit und Vorschläge für mögliche Aktionen, um sich vor neugierigen Augen zu schützen.

Weitere Informationen zur Konfiguration des Schwachstellenschutzes finden Sie im Kapitel *„Schwachstellen“* (S. 134).

**SICHERE DATEIEN**

Mit der Funktion Sichere Dateien können Sie sicherstellen, dass Ihre persönlichen Dateien vor Ransomware-Angriffen zuverlässig geschützt sind.

Weitere Informationen zur Konfiguration von Sichere Dateien zum Schutz Ihrer persönlichen Dateien vor Ransomware-Angriffen finden Sie im Kapitel *„Sichere Dateien“* (S. 145).

## Privatsphäre

Im Bereich Privatsphäre können Sie die Bitdefender-VPN-App öffnen, Ihre persönlichen Daten verschlüsseln, Ihre Online-Transaktionen schützen, Ihre Webcam und Ihr Surf-Erlebnis absichern und Ihre Kinder schützen, indem Sie Ihre Online-Aktivitäten einsehen und einschränken können.

Im Bereich Privatsphäre können Sie die folgenden Funktionen verwalten:

**VPN**

Mit VPN schützen Sie Ihre Online-Aktivitäten und verbergen Ihre IP-Adresse bei Verbindungen mit ungesicherten WLAN-Netzwerken wie zum Beispiel in Flughäfen, Einkaufszentren, Cafés oder Hotels. Darüber hinaus können Sie regionale Inhaltsbeschränkungen umgehen.

Weitere Information über diese Funktion finden Sie unter *„VPN“* (S. 161).

**VERSCHLÜSSELN**

Hiermit können Sie auf Ihrem Computer verschlüsselte und passwortgeschützte logische Laufwerke (Datentresore) anlegen, unter denen Sie Ihre vertraulichen und sensiblen Daten sicher abspeichern können.

Weitere Informationen zum Anlegen von verschlüsselten, passwortgeschützten logischen Laufwerken (Datentresore) auf Ihrem Computer finden Sie im Kapitel *„Verschlüsselung“* (S. 148).

**Webcam-Schutz**

Der Webcam-Schutz von Bitdefender schützt Ihre Webcam vor allen Gefahren, indem es den Zugriff nicht autorisierter Apps blockiert.

Weitere Informationen zum Schutz Ihrer Webcam vor Malware finden Sie im Kapitel *„Webcam-Schutz“* (S. 142).

**PASSWORTMANAGER**

Der Bitdefender-Passwortmanager hilft Ihnen, nie wieder ein Passwort zu vergessen. Zudem schützt er Ihre Privatsphäre und garantiert ein sicheres Internet-Vergnügen.

Weitere Informationen über die Konfiguration des Passwortmanagers finden Sie im Kapitel *„Passwortmanager-Schutz für Ihre Anmeldedaten“* (S. 154).

**SAFEPAY**

Mit dem Bitdefender Safepay™-Browser können Sie Ihre Online-Bankgeschäfte und -Einkäufe und alle anderen Online-Transaktionen absichern und vor fremden Zugriff schützen.

Klicken Sie im Bitdefender-Hauptfenster auf die **Safepay**-Schaltfläche, um Ihre Online-Transaktionen in einer sicheren Umgebung abzuwickeln.

Weitere Informationen zu Bitdefender Safepay finden Sie im Kapitel *„Sichere Online-Transaktionen mit Safepay“* (S. 165).

**ELTERNBERATER**

Mit dem Bitdefender-Elternberater können Sie die Computer-Nutzung Ihres Kindes jederzeit überwachen. Bei unangemessenen Inhalten können Sie den Zugriff auf das Internet und auf bestimmte Anwendungen einschränken.

Klicken Sie im Bereich Elternberater auf **Konfigurieren**, um die Geräte Ihrer Kinder zu konfigurieren und Ihre Aktivitäten von überall aus zu überwachen.

Weitere Informationen zur Konfiguration des Elternberaters finden Sie in Kapitel *„Elternberater“* (S. 171).

**DATENSCHUTZ**

Mit der Datenschutzfunktionen können Sie Dateien dauerhaft löschen. Klicken Sie unter Datenschutz auf **Dateischredder**, um einen Assistenten zu starten, mit dem Sie Dateien endgültig von Ihrem System entfernen können.

Weitere Informationen zur Konfiguration des Datenschutzes finden Sie im Kapitel *„Datenschutz“* (S. 169).

## Extras

Im Bereich Extras können Sie Ihre Systemgeschwindigkeit deutlich steigern und Ihre Geräte verwalten.

**Tune-Up**

Bitdefender Total Security 2018 bietet Ihnen nicht nur Sicherheit, sondern hilft Ihnen auch dabei, die Leistung Ihres Computers zu verbessern.

Über die Tuning-Funktion können Sie auf eine Reihe nützlicher Werkzeuge zugreifen:

- Ein-Klick-Optimierung

- Systemstart-optimierung
- Disk Cleanup

Weitere Informationen zu den Tools zur Leistungsoptimierung finden Sie im Kapitel *„Extras“ (S. 188)*.

**Diebstahlschutz**

Der Bitdefender-Diebstahlschutz schützt Ihren Computer und Ihre Daten bei Verlust oder Diebstahl. In einem solchen Fall können Sie Ihren Computer per Fernzugriff lokalisieren und sperren. Zudem können Sie alle Daten auf Ihrem System vollständig löschen.

Der Bitdefender-Diebstahlschutz bietet die folgenden Funktionen:

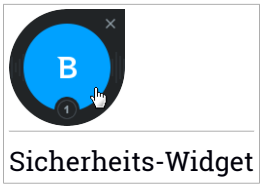
- Fernortung
- Fernsperrung
- Fernlöschung
- Fernbenachrichtigung

Weitere Informationen zum Schutz Ihres Systems vor unbefugtem Zugriff finden Sie im Kapitel *„Diebstahlschutz“ (S. 184)*.

## 2.2.4. Sicherheits-Widget

Das **Sicherheits-Widget** ist die bequemste und schnellste Art Bitdefender Total Security 2018 zu steuern. Wenn Sie dieses kleine, unauffällige Widget auf Ihren Desktop legen, haben Sie jederzeit wichtige Informationen im Blick und können zentrale Aufgaben ausführen:

- Öffnet das Bitdefender-Hauptfenster.
- Scan-Activität in Echtzeit überwachen;
- den Sicherheitsstatus Ihres Systems überwachen und gefundene Probleme beheben;
- Zeigt an, wenn ein Update durchgeführt wird.
- Benachrichtigungen und Ereignisprotokolle von Bitdefender lesen;
- Dateien und Ordner (einzeln oder als Gruppe) scannen, indem Sie sie auf das Widget ziehen;




Der Gesamtsicherheitsstatus Ihres Computers wird **in der Mitte** des Widgets angezeigt. Farbe und Form des Symbols in der Mitte zeigen unterschiedliche Status an.

Die Sicherheit Ihres Systems wird durch kritische Probleme beeinträchtigt.

Sie benötigen Ihre sofortige Aufmerksamkeit und müssen umgehend behoben werden. Klicken Sie auf das Statussymbol, um die gemeldeten Probleme zu beheben.

Die Sicherheit Ihres Systems wird durch nicht-kritische Probleme beeinträchtigt. Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben. Klicken Sie auf das Statussymbol, um die gemeldeten Probleme zu beheben.

Ihr System ist geschützt.

Während ein Bedarf-Scan läuft, wird dieses animierte Symbol angezeigt.

Wenn Probleme gemeldet werden, klicken Sie auf das Statussymbol, um den Problembehebungsassistenten zu starten.

**Im unteren Bereich** des Widgets werden die ungelesenen Ereignisse angezeigt (die Anzahl der unbeachteten Ereignisse, die Bitdefender gemeldet hat). Klicken Sie auf den Ereigniszähler, der z. B. bei einem ungelesenen Ereignis so 1 aussieht, um das Benachrichtigungsfenster zu öffnen. Weitere Informationen finden Sie im Kapitel *„Nachrichten“* (S. 16).

## Dateien und Verzeichnis scannen

Mit dem Sicherheits-Widget können Sie ganz einfach Dateien und Ordner scannen. Sie können Dateien und/oder Ordner einfach auf das **Sicherheits-Widget** ziehen und dort ablegen, um diese(n) Datei/Ordner zu scannen.

Der Viren-Scan-Assistent wird angezeigt. Er führt Sie durch den Scan-Vorgang. Die Scan-Optionen sind für bestmögliche Erkennungsraten vorkonfiguriert und können nicht verändert werden. Falls infizierte Dateien gefunden werden, wird Bitdefender versuchen, diese zu desinfizieren (den Schad-Code zu entfernen). Wenn die Desinfizierung fehlschlagen sollte, wird Ihnen der Viren-Scan-Assistent andere Möglichkeiten anbieten, wie mit den infizierten Dateien verfahren werden soll.

### Das Sicherheits-Widget ausblenden/anzeigen

Wenn Sie das Widget nicht mehr angezeigt bekommen möchten, klicken Sie einfach auf .

Verwenden Sie eine der folgenden Methoden, um das Sicherheits-Widget wiederherzustellen:

- Über die Task-Leiste:
  1. Klicken Sie mit der rechten Maustaste auf das Bitdefender-Symbol in der Task-Leiste.
  2. Klicken Sie im daraufhin angezeigten Kontextmenü auf **Sicherheits-Widget anzeigen**.
- Über die Bitdefender-Benutzeroberfläche:
  1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
  2. Wechseln Sie zum Reiter **ALLGEMEIN**.
  3. Aktivieren Sie den **Sicherheits-Widget anzeigen**, indem Sie auf den entsprechenden Schalter klicken.

Das Bitdefender-Sicherheits-Widget ist standardmäßig deaktiviert.

## 2.2.5. Aktivität

Im Aktivitätsfenster werden Informationen zu den Aktionen angezeigt, die Bitdefender in den vergangenen 30 Tagen auf Ihrem Gerät durchgeführt hat. Hier können Sie überprüfen, welche Anwendungen, Bedrohungen und Angriffe in diesem Zeitraum blockiert wurden und ob Ransomware-Angriffe stattgefunden haben.

Sie können das Aktivität-Dashboard in Bitdefender Central zudem über den entsprechenden Link aufrufen.

Mit einem Klick auf den entsprechenden Link können Sie den Sicherheitsbericht aufrufen. Hier können Sie die wöchentlichen Statusübersicht für Ihr Produkt einsehen und erhalten Tipps, wie Sie Ihren Systemschutz weiter verbessern können. Diese Tipps sind eine wichtige Hilfe bei der Verwaltung Ihres Schutzes und ermöglichen einen schnellen Überblick über die verfügbaren Aktionen.

Der Bericht wird einmal pro Woche erstellt und fasst alle relevanten Informationen zu den Produktaktivitäten zusammen, um Ihnen einen schnellen Überblick über alle Ereignisse in diesem Zeitraum zu geben.

Die Informationen im Sicherheitsbericht sind in drei Kategorien unterteilt:

- Der Bereich **Schutz** - Zeigt Informationen zum Thema Systemschutz an.
  - **Geprüfte Spy-Dateien**

    Hier sehen Sie die Dateien, die von Bitdefender im Verlauf der Woche gescannt wurden. Hier können Sie alle Details wie die Anzahl der gescannten Dateien und der von Bitdefender bereinigten Dateien einsehen.

    Weitere Informationen zum Virenschutz finden Sie im Kapitel „*Virenschutz*“ (S. 91).
  - **Gescannte Websites**

    Hier können Sie sehen, wie viele Webseiten von Bitdefender gescannt und blockiert wurden. Um Sie vor der Preisgabe von persönlichen Informationen im Internet zu schützen, sichert Bitdefender Ihren Datenverkehr ab.

    Weitere Informationen zum Internet-Schutz finden Sie im Kapitel „*Internet-Schutz*“ (S. 116)
  - **Schwachstellen**

    Hier können Sie Systemschwachstellen schnell und einfach identifizieren und beheben, um Ihren Computer besser vor Bedrohungen und Hacker-Angriffen zu schützen.

    Weitere Informationen zum Schwachstellen-Scan finden Sie im Kapitel „*Schwachstellen*“ (S. 134).
  - **Ereignischronik**

Hier können Sie sich einen Überblick über alle Scan-Prozesse und von Bitdefender im Laufe der Woche behobenen Probleme verschaffen. Die Ereignisse sind nach Tagen geordnet.

Weitere Informationen und ein detailliertes Ereignisprotokoll aller Aktivitäten auf Ihrem Computer finden Sie unter *„Nachrichten“ (S. 16)*.

- Im Bereich **Privatsphäre** erhalten Sie Informationen zum Thema Privatsphäre auf Ihrem System.
  - **Dateien im Tresor**

    Hier sehen Sie, wie viele Dateien Sie vor unbefugten Zugriff geschützt haben.

    Weitere Informationen zum Anlegen von verschlüsselten, passwortgeschützten logischen Laufwerken (Datentresore) auf Ihrem Computer finden Sie im Kapitel *„Verschlüsselung“ (S. 148)*.
- **Optimierung** - Hier erhalten Sie Informationen zu gewonnenen Speicherplatz, optimierten Anwendungen und der Akkulaufzeit, die Sie durch den Akkubetrieb gewonnen haben.
  - **Bereinigter Speicherplatz**

    Hier sehen Sie, wie viel Speicherplatz während der Systemoptimierung gewonnen wurde. Mit dem PC-Tuning verbessert Bitdefender Ihre Systemgeschwindigkeit.

    Weitere Information über das Tuning finden Sie im Kapitel *„Extras“ (S. 188)*.
  - **Gewonnene Akkulaufzeit**

    Hier können Sie sehen, wie viel Akkulaufzeit Sie durch den Akkubetrieb gewonnen haben.

    Weitere Informationen zum Akkubetriebsprofil finden Sie im Kapitel *„Akkubetriebsprofil“ (S. 198)*.
  - **Optimierte Apps**

    Hier sehen Sie die Anzahl der Apps, die Sie im Rahmen der Profile verwendet haben.

    Weitere Informationen zu den Profilen finden Sie im Kapitel *„Profile“ (S. 192)*.

## Aufrufen des Sicherheitsberichts

Der Sicherheitsbericht nutzt ein System zur Problemverfolgung, um Sicherheitsereignisse für Ihren Computer und Ihre Daten zu erkennen und Sie darüber zu informieren. Zu den gefundenen Problemen gehören auch wichtige Schutzeinstellungen, die deaktiviert sind, und andere Umstände, die ein Sicherheitsrisiko darstellen. Mithilfe des Berichts können Sie bestimmte Bitdefender-Komponenten konfigurieren oder vorbeugende Maßnahmen ergreifen, um Ihren Computer und Ihre privaten Daten zu schützen.

So können Sie den Sicherheitsbericht aufrufen:

1. Den Bericht öffnen:
   - Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.

     Klicken Sie auf den **Sicherheitsbericht**-Link unten rechts im Aktivitätsberichtfenster.
   - Rechtsklicken Sie auf das Bitdefender-Symbol in der Task-Leiste und wählen Sie **Sicherheitsbericht anzeigen**.
   - Sie erhalten eine Pop-up-Benachrichtigung sobald ein Bericht bereitsteht. Klicken Sie auf **Anzeigen**, um den Aktivitätsbericht aufzurufen.

     In Ihrem Browser wird eine Seite geöffnet, auf der Sie den erstellten Bericht einsehen können.
2. Im Fenster oben können Sie den allgemeinen Sicherheitsstatus einsehen.
3. Lesen Sie unsere Empfehlungen unten auf der Seite.

Die Farbe des Sicherheitsstatusbereichs verändert sich abhängig von den erkannten Problemen. Zudem werden unterschiedliche Meldungen angezeigt:

- **Der Bereich ist grün markiert.** Es müssen keine Probleme behoben werden. Ihr Rechner und Ihre Daten sind geschützt.
- **Der Bereich ist orange markiert.** Die Sicherheit Ihres Systems wird durch nicht-kritische Probleme beeinträchtigt. Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben.
- **Der Bereich ist rot markiert.** Die Sicherheit Ihres Systems wird durch kritische Probleme beeinträchtigt. Sie sollten sich umgehend um diese Probleme kümmern.

### Aktivieren oder Deaktivieren der Benachrichtigungen zum Sicherheitsbericht

So können Sie die Benachrichtigungen zum Sicherheitsbericht aktivieren oder deaktivieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das ⚙-Symbol.
2. Klicken Sie Fenster **ALLGEMEIN** auf den entsprechenden EIN/AUS-Schalter.

   Die Benachrichtigungen zum Sicherheitsbericht sind standardmäßig aktiviert.

## 2.3. Bitdefender Central

Bitdefender Central stellt Ihnen eine Web-Plattform zur Verfügung, über die Sie auf die Online-Funktionen und -Dienste des Produkts zugreifen und wichtige Aufgaben auf allen Geräten ausführen können, auf denen Bitdefender installiert ist. Über https://central.bitdefender.com können Sie sich mit jedem internetfähigen Computer oder Mobilgerät bei Ihrem Bitdefender-Konto anmelden. Nachdem Sie sich angemeldet haben, stehen Ihnen die folgenden Optionen zur Verfügung:

- Laden Sie Bitdefender herunter und installieren Sie es auf Windows-, macOS-, iOS- und Android-Betriebssystemen. Die folgenden Produkte stehen zum Download bereit:
  - Bitdefender Total Security 2018
  - Bitdefender Antivirus for Mac
  - Bitdefender Mobile Security für Android
  - Bitdefender Mobile Security for iOS
  - Bitdefender-Elternratgeber
- Verwaltung und Verlängerung Ihrer Bitdefender-Abonnements.
- Neue Geräte zu Ihrem Netzwerk hinzufügen und diese Geräte aus der Ferne verwalten.
- Mit dem Diebstahlschutz schützen Sie Ihre Netzwerkgeräte und die darauf gespeicherten Daten vor Verlust und Diebstahl.

- die Einstellungen des Elternberaters für die Geräte Ihrer Kinder konfigurieren und deren Aktivität auf dem Rechner überwachen, auch wenn Sie nicht zu Hause sind.
- den Aktivitätsbericht anzeigen, um den Status Ihres aktuellen Abonnements und die Geräte in Ihrem Netzwerk zu überprüfen, und wenn nötig die Leistung Ihrer Windows-Geräte aus der Ferne zu verbessern.

## So können Sie Bitdefender Central aufrufen:

Bitdefender Central kann auf verschiedene Weise aufgerufen werden. Je nach durchzuführender Aufgabe stehen Ihnen die folgenden Optionen zur Verfügung:

- Über das Bitdefender-Hauptfenster:
  1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
  2. Klicken Sie auf den **Bitdefender Central aufrufen**-Link.
  3. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Bitdefender-Konto an.
- Über Ihren Web-Browser:
  1. Öffnen Sie einen Web-Browser auf jedem beliebigen internetfähigen Gerät.
  2. Gehen Sie zu: https://central.bitdefender.com.
  3. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Bitdefender-Konto an.

### 2.3.1. Meine Abonnements

Über die Bitdefender Central-Plattform können Sie bequem die Abonnements für alle Ihre Geräte verwalten.

#### Verfügbare Abonnements anzeigen

So können Sie Ihre verfügbaren Abonnements anzeigen:

1. Rufen Sie Bitdefender Central auf.
2. Rufen Sie den Bereich **Meine Abonnements** auf.

Hier werden alle Informationen zur Verfügbarkeit Ihrer Abonnements und die Anzahl der Geräte angezeigt, auf denen diese verwendet werden.

Klicken Sie auf eine Abonnementkarte, um Ihrem Abonnement ein neues Gerät hinzuzufügen oder es zu verlängern.

**Beachten Sie**

Es ist möglich, eine oder mehrere Abonnements unter einem Benutzerkonto zu vereinen, vorausgesetzt, dass diese für verschiedene Plattformen (Windows, macOS, iOS oder Android) gültig sind.

## Ein neues Gerät hinzufügen

Falls Ihr Abonnement mehr als ein Gerät umfasst, können Sie ein neues Gerät hinzufügen und darauf Ihr Bitdefender Total Security 2018 installieren. Gehen Sie dazu wie folgt vor:

1. Rufen Sie Bitdefender Central auf.
2. Rufen Sie den Bereich **Meine Geräte** auf und klicken Sie auf **LOKALEN SCHUTZ INSTALLIEREN**.
3. Wählen Sie eine der beiden verfügbaren Optionen:
   - **HERUNTERLADEN**

     Klicken Sie auf die Schaltfläche und speichern Sie die Installationsdatei.
   - **Auf einem anderen Gerät**

     Wählen Sie **Windows** aus, um Ihr Bitdefender-Produkt herunterzuladen, und klicken Sie danach auf **FORTFAHREN**. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **ABSCHICKEN**.
4. Warten Sie, bis der Download abgeschlossen ist, und führen Sie das Installationsprogramm aus.

## Abonnement verlängern

Falls Sie sich nicht für eine automatische Verlängerung Ihres Bitdefender-Abonnements entschieden haben, können Sie es auch selbst verlängern. Gehen Sie dazu wie folgt vor:

1. Rufen Sie Bitdefender Central auf.
2. Rufen Sie den Bereich **Meine Abonnements** auf.
3. Wählen Sie die gewünschte Abonnementkarte aus.

4. Klicken Sie zum Fortfahren auf **VERLÄNGERN**.

In Ihrem Web-Browser wird eine neue Seite geöffnet, über die Sie Ihr Bitdefender-Abonnement verlängern können.

## Abonnement aktivieren

Sie können Ihr Abonnement während des Installationsvorgangs mithilfe Ihres Bitdefender-Kontos aktivieren. Der Gültigkeitszeitraum beginnt mit dem Zeitpunkt der Aktivierung.

Falls Sie einen Aktivierungscode von einem unserer Wiederverkäufer gekauft oder diesen als Geschenk erhalten haben, können Sie die Gültigkeitsdauer eines bestehenden Bitdefender-Abonnements unter diesem Benutzerkonto um diesen Zeitraum verlängern, vorausgesetzt es handelt sich um einen Code für das gleiche Produkt.

So können Sie ein Abonnement mithilfe eines Aktivierungscodes aktivieren:

1. Rufen Sie Bitdefender Central auf.
2. Rufen Sie den Bereich **Meine Abonnements** auf.
3. Klicken Sie auf **AKTIVIERUNGSCODE** und geben Sie den Code in das entsprechende Feld ein.
4. Klicken Sie zum Fortfahren auf **AKTIVIEREN**.

Das Abonnement wurde aktiviert. Rufen Sie den Bereich **Meine Geräte** auf und klicken Sie auf **LOKALEN SCHUTZ INSTALLIEREN**, um das Produkt auf einem Ihrer Geräte zu installieren.

## 2.3.2. Meine Geräte

Über Ihr Bitdefender Central können Sie im Bereich **Meine Geräte** die Bitdefender-Produkte auf Ihren Geräten verwalten, vorausgesetzt, diese sind eingeschaltet und mit dem Internet verbunden. Auf den Gerätekacheln sind der Gerätename, der Sicherheitsstatus angegeben sowie die Information, ob Sicherheitsprobleme auf Ihren Geräten bestehen.

Um eine nach Status oder Benutzer geordnete Liste mit allen Geräten anzuzeigen, klicken Sie oben rechts auf dem Bildschirm auf den Drop-down-Pfeil.

Sie können Gerätenamen vergeben, um die Geräte später leichter identifizieren zu können:

1. Rufen Sie Bitdefender Central auf.
2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie auf die gewünschte Gerätekachel und dann auf das Symbol  in der rechten oberen Ecke.
4. Tippen Sie auf **Einstellungen**.
5. Geben Sie einen neuen Namen in das Feld **Gerätename** ein und clicken Sie dann auf **SPEICHERN**.

Falls der Autopilot deaktiviert wurde, können Sie ihn mit einem Klick auf den Schalter wieder aktivieren. Klicken Sie **Speichern**, um die Einstellungen zu speichern.

Sie können für jedes Ihrer Geräte zur einfacheren Verwaltung einen Besitzer anlegen und zuordnen:

1. Rufen Sie Bitdefender Central auf.
2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie auf die gewünschte Gerätekachel und dann auf das Symbol  in der rechten oberen Ecke.
4. Wählen Sie **Profil**.
5. Klicken Sie auf **Besitzer hinzufügen** und füllen Sie dann die entsprechenden Felder aus. Passen Sie das Profil nach Bedarf an, indem Sie ein Foto hinzufügen und einen Geburtstag eingeben.
6. Klicken Sie auf **HINZUFÜGEN**, um das Profil zu speichern.
7. Wählen Sie aus der **Gerätebesitzer**-Liste den gewünschten Besitzer aus und klicken Sie auf **ZUORDNEN**.

So können Sie Bitdefender per Fernzugriff auf Ihren Geräten aktualisieren:

1. Rufen Sie Bitdefender Central auf.
2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie auf die gewünschte Gerätekachel und dann auf das Symbol  in der rechten oberen Ecke.
4. Wählen Sie **Update**.

Klicken Sie auf die entsprechende Gerätekarte, um das Gerät per Fernzugriff zu steuern oder Informationen zu Ihrem Bitdefender-Produkt auf einem bestimmten Geräte anzuzeigen.

Klicken Sie auf eine Gerätekarte, um die folgenden Reiter anzuzeigen:

- **Dashboard** . In diesem Fenster können Sie Details zum ausgewählten Gerät anzeigen, den Schutzstatus sowie den Status des Bitdefender VPN und die Zahl der blockierten Bedrohungen der letzten sieben Tage einsehen. Der Sicherheitsstatus ist grün, wenn es keine Sicherheitsprobleme gibt, gelb, wenn es etwas gibt, was Ihre Aufmerksamkeit erfordert, und rot, wenn Ihr Gerät gefährdet ist. Gibt es Probleme, die sich auf Ihr Gerät auswirken, klicken Sie im oberen Statusbereich auf den Drop-down-File, um weitere Details anzuzeigen. Von hier aus können die Probleme, die Ihre Gerätesicherheit beeinträchtigen, manuell behoben werden.
- **Schutz**. Über dieses Fenster können Sie per Fernzugriff einen Quick Scan oder eine Systemprüfung veranlassen. Klicken Sie auf **SCAN**, um den Vorgang zu starten. Sie können auch nachvollziehen, wann der letzte Scan auf dem Gerät durchgeführt wurde, und einen Bericht für den aktuellsten Scan abrufen, in dem die wichtigsten Informationen zusammengefasst werden.Weitere Informationen zu diesen Scan-Optionen finden Sie in den Kapiteln *„Durchführen von System-Scans“* (S. 99) und *„Durchführen von Quick Scans“* (S. 98).
- **Optimierung**. Hierüber können Sie die Leistung eines Gerätes per Fernzugriff optimieren, indem Sie es nach nicht benötigten Dateien durchsuchen, diese aufspüren und entfernen. Klicken Sie auf **START** und wählen Sie die Bereiche aus, die Sie optimieren möchten. Klicken Sie erneut auf **START**, um den Optimierungsvorgang zu starten. Klicken Sie auf den Link **Mehr ...**, um einen detaillierten Bericht zu den behobenen Problemen aufzurufen.

  Darüber hinaus können Sie die Startgeschwindigkeit Ihres Gerätes verbessern, indem Sie die Anwendungen identifizieren, die einen hohen Ressourcenverbrauch haben. Klicken Sie auf **MEHR ...** und entscheiden Sie, wie mit den gefundenen Anwendungen verfahren werden soll. Weitere Informationen zu diesen Funktionen finden Sie in den Kapiteln *„Optimierung der Systemgeschwindigkeit mit nur einem Klick“* (S. 188) und *„Optimieren der Systemstartzeit“* (S. 189).
- **Diebstahlschutz**. Falls Sie Ihr Gerät verlegt bzw. verloren haben oder es Ihnen gestohlen wurde, können Sie es mithilfe des Diebstahlschutzes orten

und per Fernzugriff steuern. Klicken Sie auf **ORTEN**, um den Standort Ihres Gerätes zu ermitteln. Die letzte bekannte Position wird mit Datum und Tageszeit angezeigt. Weitere Informationen zu dieser Funktion finden Sie unter *„Diebstahlschutz“* (S. 184).

- **Schwachstelle**. Über die **SCAN**-Schaltfläche im Reiter Schwachstellen können Sie ein Gerät auf Schwachstellen, fehlende Windows-Updates, veraltete Anwendungen oder unsichere Passwörter überprüfen. Schwachstellen können nicht per Fernzugriff behoben werden. Falls eine Schwachstelle gefunden wird, müssen Sie auf dem Gerät einen neuen Scan starten und danach den Empfehlungen folgen. Klicken Sie auf **Mehr...**, um einen detaillierten Bericht zu den gefundenen Problemen aufzurufen. Weitere Informationen zu dieser Funktion finden Sie unter *„Schwachstellen“* (S. 134).

## 2.3.3. Aktivität

Der Aktivitätsbereich in Bitdefender Central steht nur Nutzern zur Verfügung, die ein Bitdefender Family Pack 2018- oder Bitdefender Total Security Multi-Device 2018-Abonnement mit Ihren Benutzerkonten verknüpft haben. Hier können Sie einsehen, wie Bitdefender die Geräte, auf denen es installiert ist, in den letzten sieben Tagen geschützt hat. Sie erhalten zudem Informationen über das enthaltene Abonnement.

Im Fenster **AKTIVITÄT** können Sie auf die folgenden Karten zugreifen:

- **Schutz**. Hier finden Sie Informationen über Dateien, Anwendungen und URLs, die aufgrund Ihres verdächtigen Verhaltens blockiert wurden. Um Ihnen zu zeigen, wann Probleme aufgetreten sind, stehen Ihnen Diagramme zur Auswahl, in denen die gesammelten Daten nach Tagen und der Anzahl der gefundenen Bedrohungen sortiert sind. Sie können zudem Ihren Mauszeiger über die angezeigten Daten bewegen, um die Anzahl der gefundenen Bedrohungen zu erfahren.

  Unten auf der Karte finden Sie den Namen des Geräts mit der höchsten Anzahl der Bedrohungen.

- **Tune Up**. Von hier aus können Sie die Leistungsfähigkeit aller Windows-Geräte optimieren, auf denen das Bitdefender Total Security 2018-Produkt installiert ist. Die angezeigten Informationen basieren auf der Funktion Systemstartoptimierung. Diese zeigt an, welche Anwendungen bei Systemstart ausgeführt werden und ermöglicht Ihnen, ihr Verhalten bei diesem Schritt zu verwalten. Abhängig davon, wie sich andere Nutzer

bei der Anwendung des **Verzögern**-Befehls entschieden haben, werden nur die ersten drei Geräte angezeigt. Klicken Sie auf **Anwenden**, um die vorgeschlagenen Änderungen auf dem ausgewählten Gerät durchzuführen.

Klicken Sie auf den Link, der die Anzahl der gefundenen Anwendungen und die eingesparte Zeit anzeigt, um die Entscheidungen anderer Bitdefender-Nutzer zu sehen. Es werden Details zur Startzeit Ihres Systems, zur Startzeit Ihrer Apps beim Systemstart und zur eingesparten Zeit angezeigt. Wählen Sie **ALLE VERZÖGERN** aus, wenn sie beim Systemstart nicht mehr ausgeführt werden sollen. Weitere Informationen zur Bitdefender-Systemstartoptimierung finden Sie im Kapitel *„Optimieren der Systemstartzeit“ (S. 189)*.

> **Beachten Sie**
> Falls auf Ihren Windows-Geräten der Bitdefender-Schutz nicht installiert wurde, enthält die **Tune Up**-Karte auch keine Informationen.

- **Abonnement**. Hier können Sie sehen, wie viele Geräte durch Ihr Abonnement abgedeckt sind und auf wie vielen Geräten Sie den Bitdefender-Schutz installiert haben. Um Bitdefender auf anderen Geräten zu installieren, klicken Sie auf die **INSTALLIEREN**-Schaltfläche unter dem gewünschten Betriebssystem. Führen Sie danach die erforderlichen Schritte durch.

  Der Name des genutzten Abonnements wird mit einem farbigen Punkt angezeigt:

  - Lila - Ihr Abonnement ist aktiv.
  - Rot - Ihr Abonnement wird in Kürze ablaufen. Wir empfehlen, es so schnell wie möglich zu verlängern, damit Ihre Geräte auch weiterhin geschützt bleiben.

  Klicken Sie auf **Weitere Details**, um zur **Abonnement**-Seite weitergeleitet zu werden. Hier können Sie detaillierte Informationen über Ihr aktives Abonnement einsehen.

## 2.3.4. Mein Konto

Im Bereich **Mein Konto** können Sie Ihr Profil anpassen, Ihr Passwort ändern sowie die Benutzersitzungen und die Hilfemeldungen von Bitdefender Central verwalten.

Klicken Sie auf das -Symbol oben rechts auf dem Bildschirm und wählen Sie **Mein Konto**, um auf die folgenden Reiter zuzugreifen:

- **Profil** - hier können Sie Kontoinformationen hinzufügen und bearbeiten.
- **Passwort ändern** - hier können Sie das Passwort Ihres Kontos ändern.
- **Sitzungsverwaltung** - hier können Sie die jüngsten inaktiven und aktiven Benutzersitzungen auf mit Ihrem Konto verbundenen Geräten verwalten.
- **Einstellungen** - hier können Sie die Hilfemeldungen von Bitdefender Central ein- und ausschalten und einstellen, ob Sie benachrichtigt werden möchten, wenn mit Ihren Android-Geräten Fotos gemacht werden.

### 2.3.5. Nachrichten

Über das -Symbol bleiben Sie immer auf dem Laufenden, was auf den mit Ihrem Konto verbundenen Geräten passiert. Ein Klick auf dieses Symbol gibt Ihnen einen groben Überblick über die Aktivitäten der Bitdefender-Produkte, die auf Ihren Geräten installiert sind.

## 2.4. Bitdefender auf dem neuesten Stand halten

Jeden Tag werden neue Bedrohungen entdeckt und identifiziert. Darum ist so wichtig, dass Bitdefender jederzeit über die neuesten Bedrohungsinformationen verfügt.

Falls Sie über eine Breitbandverbindung oder eine DSL-Verbindung verfügen, arbeitet Bitdefender eigenständig. Standardmäßig sucht die Software nach Updates, wenn Sie Ihren Computer einschalten und danach einmal pro **Stunde**. Wenn ein neues Update erkannt wird, wird es automatisch auf Ihren PC heruntergeladen und installiert.

Der Updatevorgang wird "on the fly" durchgeführt. Das bedeutet, dass die entsprechenden Dateien stufenweise aktualisiert werden. So stört der Update-Vorgang nicht den Betrieb des Produkts, während gleichzeitig alle Schwachstellen behoben werden.

**Wichtig**
Um immer vor den neuesten Bedrohungen geschützt zu sein, sollte das automatische Update immer aktiviert bleiben.

In manchen Situationen kann es notwendig werden, dass Sie eingreifen, um den Bitdefender-Schutz auf dem neuesten Stand zu halten:

- Wenn Ihr Computer über einen Proxy-Server mit dem Internet verbunden ist, müssen Sie die Proxy-Einstellungen wie unter *„Wie konfiguriere ich Bitdefender für die Nutzung einer Proxy-Verbindung?“* (S. 85) beschrieben konfigurieren.
- Bei einer langsamen Internetverbindung können Fehler beim Herunterladen von Updates auftreten. Eine Anleitung zur Behebung solcher Fehler finden Sie im Kapitel *„Wie man Bitdefender-Updates auch mit einer langsamen Internet-Verbindung durchführen kann“* (S. 211).
- Falls Sie sich per Einwahl mit dem Internet verbinden, ist es sinnvoll, regelmäßig ein manuelles Bitdefender-Update durchzuführen. Weitere Informationen finden Sie unter *„Durchführung eines Updates“* (S. 47).

### 2.4.1. Überprüfen, ob Bitdefender auf dem neuesten Stand ist

Links im Statusbereich wird unter **Sicherheitstatus** der Zeitpunkt des letzten Bitdefender-Updates angezeigt.

Um ausführliche Informationen zu Ihren letzten Updates zu erhalten, rufen Sie die Update-Ereignisse auf:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wählen Sie unter dem Reiter **Alle** die Benachrichtigung bezüglich des neuesten Updates aus.

Sie können herausfinden, wann Updates angestoßen wurden und weitere Informationen dazu einholen (d.h. ob sie erfolgreich waren oder nicht, ob ein Neustart erforderlich ist, um die Installation abzuschließen). Falls nötig starten Sie das System sobald es Ihnen möglich ist neu.

### 2.4.2. Durchführung eines Updates

Sie benötigen eine Internet-Verbindung, um Updates durchzuführen.

Sie haben folgende Möglichkeiten, ein Update zu starten:

- Öffnen Sie die Bitdefender-Benutzeroberfläche und klicken Sie auf den **JETZT AKTUALISIEREN**-Link, der sich unterhalb Ihres Programmstatus befindet.

- Rechtsklicken Sie in der Task-Leiste auf das Bitdefender-Symbol und wählen Sie **Jetzt aktualisieren**.

Die Funktion Update stellt eine Verbindung mit dem Bitdefender-Update-Server her und sucht nach verfügbaren Updates. Wenn ein Update erkannt wird, werden Sie abhängig von den Update-Einstellungen entweder aufgefordert, dies zu bestätigen oder das Update wird automatisch durchgeführt.

**Wichtig**
Möglicherweise kann ein Neustart nach dem vollständig durchgeführten Update notwendig werden. Wir empfehlen, das so bald wie möglich zu tun.

Sie können die Updates auf Ihren Geräten zudem per Fernzugriff vornehmen, vorausgesetzt, sie sind eingeschaltet und mit dem Internet verbunden.

So können Sie Bitdefender per Fernzugriff auf Ihren Geräten aktualisieren:

1. Rufen Sie Bitdefender Central auf.
2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie auf die gewünschte Gerätekachel und dann auf das Symbol ⋮ in der rechten oberen Ecke.
4. Wählen Sie **Update**.

## 2.4.3. Aktivieren / Deaktivieren der automatischen Updates

So können Sie automatische Updates aktivieren oder deaktivieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das ⚙-Symbol.
2. Wechseln Sie zum Reiter **UPDATE**.
3. Klicken Sie auf die entsprechenden EIN/AUS-Schalter.
4. Ein Warnung wird angezeigt. Sie müssen Ihre Auswahl bestätigen, indem Sie im Menü wählen, wie lange die automatischen Updates deaktiviert bleiben sollen. Sie können automatische Updates für 5, 15 oder 30 Minuten, 1 Stunde, dauerhaft oder bis zum Neustart des Systems deaktivieren.

**Warnung**
Hierbei handelt es sich um ein grobes Sicherheitsrisiko. Wir empfehlen, die automatischen Updates so kurz wie möglich zu deaktivieren. Denn Bitdefender kann Sie nur dann gegen die neusten Bedrohungen schützen, wenn es auf dem neuesten Stand ist.

## 2.4.4. Update-Einstellungen anpassen

Updates können im lokalen Netzwerk, über das Internet, direkt oder durch einen Proxy-Server durchgeführt werden. Standardmäßig scannt Bitdefender jede Stunde auf neue Updates und installiert diese ohne Ihr Zutun.

Die standardmäßigen Update-Einstellungen eignen sich für die meisten Benutzer und es ist normalerweise nicht erforderlich, diese zu ändern.

So können Sie die Update-Einstellungen anpassen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das ⚙-Symbol.
2. Wechseln Sie zum Reiter **UPDATE** und passen Sie die Einstellungen nach Ihren Wünschen an.

### Update-Häufigkeit

Bitdefender ist für eine stündliche Update-Prüfung konfiguriert. Die Update-Häufigkeit lässt sich durch Schieben des entsprechenden Reglers auf den gewünschten Update-Zeitraum festlegen.

### Update-Server

Bitdefender ist so konfiguriert, dass Updates von den Bitdefender-Update-Servern aus dem Internet heruntergeladen werden. Die Update-Adresse ist eine generische Internetadresse, die automatisch zu dem Bitdefender-Update-Server, der sich am nächsten zu Ihrem Standort befindet, umgeleitet wird.

Verändern Sie die Update-Adresse nicht, es sei denn, Sie werden von einem Bitdefender-Mitarbeiter oder Ihrem Netzwerkadministrator (falls Sie mit einem Unternehmensnetzwerk verbunden sind) ausdrücklich dazu aufgefordert.

Klicken Sie auf **STANDARD**, um die ursprüngliche Update-Adresse wiederherzustellen.

### Update-Verarbeitungsregeln

Es gibt drei Möglichkeiten, Updates herunterzuladen und zu installieren:

- **Update im Hintergrund** - Bitdefender Updates werden automatisch heruntergeladen und installiert.
- **Vor dem Download nachfragen** - Sobald ein Update verfügbar ist, werden Sie gefragt, ob es heruntergeladen werden soll.
- **Vor der Installation nachfragen** - Sobald ein Update heruntergeladen wurde, werden Sie gefragt, ob die Installation durchgeführt werden soll.

Manche Updates erfordern einen Neustart, um die Installation abzuschließen. Sollte ein Update einen Neustart erforderlich machen, arbeitet Bitdefender standardmäßig mit den alten Dateien weiter, bis der Benutzer den Computer aus eigenen Stücken neu startet. Dadurch soll verhindert werden, dass der Update-Prozess von Bitdefender den Benutzer in seiner Arbeit behindert.

Wenn Sie eine Meldung erhalten möchten, sobald ein Update einen Neustart erfordert, deaktivieren Sie die Option **Neustart verschieben**, indem Sie auf den entsprechenden Schalter klicken.

## 2.4.5. Regelmäßige Updates

Um sicherzustellen, dass Sie immer mit der neuesten Version arbeiten, sucht Ihr Bitdefender automatisch nach Produktupdates. Diese Updates können neue Funktionen und Verbesserungen beinhalten, Produktprobleme beheben und automatische Upgrades auf eine neue Version umfassen. Wird eine neue Bitdefender-Version per Update ausgeliefert, werden benutzerdefinierte Einstellungen gespeichert und der Vorgang der De- und Neuinstallation wird übersprungen.

Diese Updates erfordern einen Neustart des Systems, um die Installation neuer Dateien zu initiieren. Ein Pop-up-Fenster fordert Sie auf das System neu zu starten, sobald das Update abgeschlossen wurde. Sollten Sie diese Benachrichtigung verpasst haben, können Sie im Fenster Benachrichtigungen beim Eintrag über das neueste Update auf **JETZT NEU STARTEN** klicken oder das System manuell neu starten.

**Beachten Sie**

Die Updates mit neuen Funktionen und Verbesserungen sind Benutzern vorbehalten, bei denen Bitdefender 2017 installiert ist.

# 3. GEWUSST WIE

## 3.1. Installation

### 3.1.1. Wie installiere ich Bitdefender auf einem zweiten Computer?

Falls Ihr erworbenes Abonnement für mehrere Geräte gültig ist, können Sie über Ihr Bitdefender-Konto einen zweiten PC aktivieren.

So können Sie Bitdefender auf einem zweiten Computer installieren:

1. Klinken Sie unten rechts in der Bitdefender-Benutzeroberfläche auf den Link **AUF EINEM ANDEREN GERÄT INSTALLIEREN**.

   Sie werden auf die Bitdefender-Konto Website weitergeleitet. Stellen Sie sicher, dass Sie sich mit Ihren Anmeldedaten angemeldet haben.

2. Wählen Sie im angezeigten Fenster das gewünschte Betriebssystem und klicken Sie dann auf **FORTFAHREN**.

3. Geben Sie die E-Mail-Adresse ein, an die wir den Download-Link für die Installation auf der gewählten Plattform senden sollen.

4. Führen Sie das von Ihnen heruntergeladene Bitdefender aus. Warten Sie, bis die Registrierung abgeschlossen ist und schließen Sie dann das Fenster.

Das neue Gerät, auf dem Sie das Bitdefender-Produkt installiert haben, wird ab sofort im Bitdefender Central-Dashboard angezeigt.

### 3.1.2. Wie kann ich Bitdefender neu installieren?

Die Folgenden sind typische Situationen, in denen Sie Bitdefender erneut installieren müssen:

- Sie haben das Betriebssystem neu installiert..
- Sie möchten Probleme beheben, die das System verlangsamt oder zum Absturz gebracht haben könnten.
- Ihr Bitdefender-Produkt startet nicht oder funktioniert nicht ordnungsgemäß.

Falls eine der genannten Situationen auf Sie zutrifft, gehen Sie bitte folgendermaßen vor:

- In **Windows 7**:
  1. Klicken Sie auf **Start** und **Alle Programme**.
  2. Suchen Sie **Bitdefender Total Security 2018** und wählen Sie **Deinstallieren**.
  3. Klicken Sie im angezeigten Fenster auf **NEU INSTALLIEREN**.
  4. Sie müssen den Computern neu starten, um den Vorgang abzuschließen.
- In **Windows 8 und Windows 8.1**:
  1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
  2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
  3. Suchen Sie **Bitdefender Total Security 2018** und wählen Sie **Deinstallieren**.
  4. Klicken Sie im angezeigten Fenster auf **NEU INSTALLIEREN**.
  5. Sie müssen den Computern neu starten, um den Vorgang abzuschließen.
- In **Windows 10**:
  1. Klicken Sie auf **Start** und danach auf Einstellungen.
  2. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie **Apps & Funktionen** aus.
  3. Suchen Sie **Bitdefender Total Security 2018** und wählen Sie **Deinstallieren**.
  4. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.
  5. Klicken Sie auf **NEU INSTALLIEREN**.
  6. Sie müssen den Computern neu starten, um den Vorgang abzuschließen.

### Beachten Sie

Wenn Sie bei der Neuinstallation wie hier beschrieben vorgehen, werden Ihre benutzerdefinierte Einstellungen gespeichert und sind im neu installierten Produkt wieder verfügbar. Weitere Einstellungen werden unter Umständen wieder auf die Standardkonfiguration zurückgesetzt.

## 3.1.3. Wo kann ich mein Bitdefender-Produkt herunterladen?

Sie können Bitdefender vom Installationsdatenträger installieren oder den Web-Installer verwenden, der über die Bitdefender Central-Plattform heruntergeladen werden kann.

**Beachten Sie**
Bevor Sie das Installationspaket ausführen, sollten Sie jede andere auf Ihrem System installierte Sicherheitslösung entfernen. Wenn Sie mehr als eine Sicherheitslösung auf Ihrem Computer verwenden, wird dadurch das System instabil.

So können Sie Bitdefender über Bitdefender Central installieren:

1. Rufen Sie Bitdefender Central auf.
2. Rufen Sie den Bereich **Meine Geräte** auf und klicken Sie auf **LOKALEN SCHUTZ INSTALLIEREN**.
3. Wählen Sie eine der beiden verfügbaren Optionen:
   - **HERUNTERLADEN**

     Klicken Sie auf die Schaltfläche und speichern Sie die Installationsdatei.
   - **Auf einem anderen Gerät**

     Wählen Sie **Windows** aus, um Ihr Bitdefender-Produkt herunterzuladen, und klicken Sie danach auf **FORTFAHREN**. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **ABSCHICKEN**.
4. Führen Sie das von Ihnen heruntergeladene Bitdefender aus.

## 3.1.4. Wie kann ich die Sprache für mein Bitdefender ändern?

Wenn Sie Bitdefender in einer anderen Sprache nutzen möchten, müssen Sie das Produkt in der entsprechenden Sprache neu installieren.

So können Sie das Bitdefender in einer anderen Sprache nutzen:

1. Entfernen Sie Bitdefender, indem Sie wie folgt vorgehen:
   - In **Windows 7**:
     a. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.

b. Suchen Sie **Bitdefender Total Security 2018** und wählen Sie **Deinstallieren**.

c. Klicken Sie im angezeigten Fenster auf **Entfernen**.

d. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.

- In **Windows 8 und Windows 8.1**:

  a. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.

  b. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.

  c. Suchen Sie **Bitdefender Total Security 2018** und wählen Sie **Deinstallieren**.

  d. Klicken Sie im angezeigten Fenster auf **Entfernen**.

  e. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.

- In **Windows 10**:

  a. Klicken Sie auf **Start** und danach auf Einstellungen.

  b. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie danach auf **Installierte Anwendungen**.

  c. Suchen Sie **Bitdefender Total Security 2018** und wählen Sie **Deinstallieren**.

  d. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.

  e. Klicken Sie im angezeigten Fenster auf **Entfernen**.

  f. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.

2. Ändern Sie die Sprache der Bitdefender Central-Benutzeroberfläche:

   a. Rufen Sie Bitdefender Central auf.

   b. Klicken Sie auf das -Symbol in der rechten oberen Bildschirmecke.

   c. Klicken Sie im Menü auf **Mein Konto**.

   d. Wechseln Sie zum Reiter **Profile**.

e. Wählen Sie eine Sprache aus der **Sprache**-Dropdown-Liste aus und klicken Sie auf **SPEICHERN**.

3. Laden Sie die Installationsdatei herunter:

   a. Rufen Sie den Bereich **Meine Geräte** auf und klicken Sie auf **LOKALEN SCHUTZ INSTALLIEREN**.

   b. Wählen Sie eine der beiden verfügbaren Optionen:

   - **HERUNTERLADEN**

     Klicken Sie auf die Schaltfläche und speichern Sie die Installationsdatei.

   - **Auf einem anderen Gerät**

     Wählen Sie **Windows** aus, um Ihr Bitdefender-Produkt herunterzuladen, und klicken Sie danach auf **FORTFAHREN**. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **ABSCHICKEN**.

4. Führen Sie das von Ihnen heruntergeladene Bitdefender aus.

**Beachten Sie**
Wenn Sie bei der Neuinstallation so vorgehen, werden die benutzerdefinierten Einstellungen endgültig gelöscht.

## 3.1.5. Wie verfahre ich mit meinem Bitdefender-Abonnement nach einem Windows-Upgrade?

Diese Situation tritt ein, wenn Sie Ihr Betriebssystem aktualisieren und Sie Ihren Bitdefender-Abonnement weiterhin nutzen möchten.

**Sollten Sie eine vorausgegangene Bitdefender-Version nutzen, können Sie ein kostenloses Upgrade auf die neueste Version von Bitdefender wie folgt durchführen:**

- Von einer Vorgängerversion von Bitdefender Antivirus auf die aktuelle Version von Bitdefender Antivirus.
- Von einer Vorgängerversion von Bitdefender Internet Security auf die aktuelle Version von Bitdefender Internet Security.
- Von einer Vorgängerversion von Bitdefender Total Security auf die aktuelle Version von Bitdefender Total Security.

**Hierbei gibt es 2 Szenarien**:

- Sie haben Ihr Betriebssystem über Windows Update aktualisiert und bemerken, dass Bitdefender nicht mehr funktioniert.

  In diesem Fall müssen Sie das Produkt wie folgt neu installieren:

  - In **Windows 7**:

    1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
    2. Suchen Sie **Bitdefender Total Security 2018** und wählen Sie **Deinstallieren**.
    3. Klicken Sie im angezeigten Fenster auf **NEU INSTALLIEREN**.
    4. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.

       Öffnen Sie die Benutzeroberfläche Ihres neu installierten Bitdefender-Produkts, um auf die Funktionen zugreifen zu können.

  - In **Windows 8 und Windows 8.1**:

    1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
    2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
    3. Suchen Sie **Bitdefender Total Security 2018** und wählen Sie **Deinstallieren**.
    4. Klicken Sie im angezeigten Fenster auf **NEU INSTALLIEREN**.
    5. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.

       Öffnen Sie die Benutzeroberfläche Ihres neu installierten Bitdefender-Produkts, um auf die Funktionen zugreifen zu können.

  - In **Windows 10**:

    1. Klicken Sie auf **Start** und danach auf Einstellungen.
    2. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie danach auf **Installierte Anwendungen**.

3. Suchen Sie **Bitdefender Total Security 2018** und wählen Sie **Deinstallieren**.
4. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.
5. Klicken Sie im angezeigten Fenster auf **NEU INSTALLIEREN**.
6. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.

   Öffnen Sie die Benutzeroberfläche Ihres neu installierten Bitdefender-Produkts, um auf die Funktionen zugreifen zu können.

**Beachten Sie**
Wenn Sie bei der Neuinstallation wie hier beschrieben vorgehen, werden Ihre benutzerdefinierte Einstellungen gespeichert und sind im neu installierten Produkt wieder verfügbar. Weitere Einstellungen werden unter Umständen wieder auf die Standardkonfiguration zurückgesetzt.

- Sie haben Ihr System gewechselt und möchten nicht auf den Bitdefender-Schutz verzichten. Deshalb müssen Sie das Produkt in der aktuellsten Version erneut installieren.

  Verfahren Sie in einer solchen Situation wie folgt:

  1. Laden Sie die Installationsdatei herunter:
     a. Rufen Sie Bitdefender Central auf.
     b. Rufen Sie den Bereich **Meine Geräte** auf und klicken Sie auf **LOKALEN SCHUTZ INSTALLIEREN**.
     c. Wählen Sie eine der beiden verfügbaren Optionen:
        - **HERUNTERLADEN**

          Klicken Sie auf die Schaltfläche und speichern Sie die Installationsdatei.
        - **Auf einem anderen Gerät**

          Wählen Sie **Windows** aus, um Ihr Bitdefender-Produkt herunterzuladen, und klicken Sie danach auf **FORTFAHREN**. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **ABSCHICKEN**.
  2. Führen Sie das von Ihnen heruntergeladene Bitdefender aus.

Weitere Information zum Bitdefender-Installationsprozess finden Sie im Kapitel *„Installation von Bitdefender Antivirus for Mac“* (S. 236).

### 3.1.6. Wie kann ich ein Upgrade auf die neueste Bitdefender-Version durchführen?

Ab Bitdefender 2018 ist ein Upgrade auf die neueste Produktversion auch ohne vorherige manuelle Deinstallation und Neuinstallation möglich. Genauer gesagt wird das neue Produkt mit allen neuen Funktionen und wesentlichen Verbesserungen als Produktupdate ausgeliefert. Wenn Sie bereits über ein aktives Bitdefender-Abonnement verfügen, wird das Produkt automatisch aktiviert.

Als Benutzer der 2017er-Version können Sie folgendermaßen vorgehen, um ein Upgrade auf die neueste Version durchzuführen:

1. Klicken Sie in der Benachrichtigung, die mit der Upgradeinfomration einhergeht, auf **JETZT NEU STARTEN**. Sollten Sie sie verpasst haben, rufen Sie das Fenster Benachrichtigungen auf, bewegen Sie den Mauszeiger auf das neueste Update und klicken Sie danach auf **JETZT NEU STARTEN**. Warten Sie, bis der Computer neu gestartet wurde.

   Das Fenster **Was gibt es Neues** mit Informationen über die verbesserten und neuen Funktionen wird angezeigt.

2. Klicken Sie auf die **Lesen Sie mehr**-Links für weitere Informationen und hilfreiche Artikel.

3. Schließen Sie das Fenster **Was gibt es Neues**, um auf die Benutzeroberfläche der neu installierten Version zuzugreifen.

Benutzer, die ein kostenloses Upgrade von Bitdefender 2016 oder einer Vorgängerversion auf die neueste Bitdefender-Version durchführen möchten, müssen zunächst die aktuelle Version über die Systemsteuerung entfernen und danach die aktuellste Installationsdatei über die Bitdefender-Website herunterladen: http://www.bitdefender.de/Downloads/. Für die Aktivierung wird ein gültiges Abonnement benötigt.

## 3.2. Abonnements

### 3.2.1. Wie kann ich mein Bitdefender-Abonnement mithilfe eines Lizenzschlüssels aktivieren?

Es gibt zwei Möglichkeiten, einen gültigen Lizenzschlüssel zur Aktivierung eines Bitdefender Total Security 2018-Abonnements zu verwenden:

- Im Falle eines Upgrades auf die neueste Bitdefender-Version:
  1. Nach Abschluss des Bitdefender Total Security 2018-Upgrades werden Sie aufgefordert, sich bei Ihrem Bitdefender-Konto anzumelden.
  2. Klicken Sie auf **Anmelden** und geben Sie die E-Mail-Adresse und das Passwort für Ihr Bitdefender-Benutzerkonto ein.
  3. Klicken Sie zum Fortfahren auf **ANMELDEN**.
  4. In Ihrem Benutzerkonto wird eine Meldung angezeigt, die die Anlage des Abonnements bestätigt. Das neu angelegte Abonnement ist für die verbleibende Gültigkeitsdauer Ihres Lizenzschlüssels und für die gleiche Anzahl an Benutzern gültig.

     Auf allen Geräten, die noch alte Bitdefender-Versionen nutzen und die mit dem Lizenzschlüssel registriert wurden, der nun in ein Abonnement umgewandelt wurde, muss das Produkt mit dem gleichen Bitdefender-Konto aktiviert werden.
- Im Falle, dass Bitdefender bisher noch nicht auf dem System installiert war:
  1. Nach Abschluss des Installationsvorgangs werden Sie aufgefordert, sich bei Ihrem Bitdefender-Konto anzumelden.
  2. Klicken Sie auf **Anmelden** und geben Sie die E-Mail-Adresse und das Passwort für Ihr Bitdefender-Benutzerkonto ein.
  3. Klicken Sie auf **ANMELDEN**, um fortzufahren, und danach auf **FERTIGSTELLEN**, um auf die Bitdefender Total Security 2018-Benutzeroberfläche zuzugreifen.
  4. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
  5. Klicken Sie auf den Link **Code aktivieren**.

Ein neues Fenster wird angezeigt.

6. Klicken Sie auf den **Holen Sie sich jetzt Ihr KOSTENLOSES Upgrade!**-Link.
7. Geben Sie Ihren Lizenzschlüssel in das entsprechende Feld ein und klicken Sie auf **MEIN PRODUKT UPGRADEN**. Ein Abonnement mit der gleichen Gültigkeitsdauer und Anzahl an Benutzern wie Ihr Lizenzschlüssel wird mit Ihrem Benutzerkonto verknüpft.

## 3.3. Bitdefender Central

### 3.3.1. Wie melde ich mit einem anderen Benutzerkonto bei Bitdefender Central an?

Sie haben ein neues Bitdefender-Konto angelegt und möchten es von nun an nutzen.

So können Sie ein weiteres Benutzerkonto nutzen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das ⓪-Symbol.
2. Klicken Sie auf **KONTO WECHSELN**, um den Computer mit einem anderen Benutzerkonto zu verknüpfen.
3. Geben Sie die E-Mail-Adresse und das Kennwort Ihres Kontos in die entsprechenden Felder ein und klicken Sie auf **EINLOGGEN**.

**Beachten Sie**

Das Bitdefender-Produkt auf Ihrem Gerät wird entsprechend dem mit Ihrem neuen Bitdefender-Konto verknüpften Abonnement automatisch umgestellt. Falls mit dem neuen Bitdefender-Konto kein verfügbares Abonnement verknüpft ist oder Sie es von einem früheren Benutzerkonto übernehmen möchten, können Sie sich wie in Kapitel *„Hilfe anfordern“* (S. 341) beschrieben mit dem Bitdefender-Support in Verbindung setzen.

### 3.3.2. Wie kann ich die Bitdefender Central-Hilfemeldungen deaktivieren?

Die Hilfemeldungen werden im Dashboard angezeigt, um Ihnen zu zeigen, wie Sie die verschiedenen Optionen in Bitdefender Central nutzen können.

So können Sie diese Meldungen deaktivieren:

1. Rufen Sie Bitdefender Central auf.
2. Klicken Sie auf das -Symbol in der rechten oberen Bildschirmecke.
3. Klicken Sie im Menü auf **Mein Konto**.
4. Wechseln Sie zum Reiter **Einstellungen**.
5. Deaktivieren Sie die Option **Hilfemeldungen aktivieren/deaktivieren**.

### 3.3.3. Ich habe das Passwort vergessen, das ich für mein Bitdefender-Konto festgelegt habe. Wie kann ich es zurücksetzen?

Das Passwort für Ihr Bitdefender-Konto können Sie auf eine von zwei Arten ändern:

- Über die Bitdefender-Benutzeroberfläche:
  1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
  2. Klicken Sie auf die Schaltfläche **KONTO WECHSELN**.

     Ein neues Fenster wird angezeigt.
  3. Klicken Sie auf den Link **Mein Passwort vergessen**.
  4. Geben Sie die E-Mail-Adresse ein, mit der Sie Ihr Bitdefender-Konto angelegt haben, und klicken Sie auf **PASSWORT VERGESSEN**.
  5. Rufen Sie Ihre E-Mails ab und klicken Sie auf die entsprechende Schaltfläche.

     Das Fenster Bitdefender PASSWORT ZURÜCKSETZEN wird angezeigt.
  6. Geben Sie Ihre E-Mail-Adresse und das neue Passwort in das entsprechende Feld ein. Das Passwort muss mindestens 8 Zeichen lang sein und Zahlen enthalten.
  7. Klicken Sie auf **PASSWORT ZURÜCKSETZEN**.
- Über Ihren Web-Browser:
  1. Gehen Sie zu: https://central.bitdefender.com.
  2. Klicken Sie auf den Link **Mein Passwort vergessen**.
  3. Geben Sie Ihre E-Mail-Adresse ein und klicken Sie danach auf **PASSWORT VERGESSEN**.

4. Rufen Sie Ihre E-Mails ab und folgen Sie der Anleitung, um ein neues Passwort für Ihr Bitdefender-Konto festzulegen.

Geben Sie von jetzt an Ihre E-Mail-Adresse und das neue Passwort ein, um auf Ihr Bitdefender-Konto zuzugreifen.

### 3.3.4. Wie kann ich die Benutzersitzungen in meinem Bitdefender-Konto verwalten?

In Ihrem Bitdefender-Konto können Sie die jüngsten inaktiven und aktiven Benutzersitzungen auf mit Ihrem Konto verbundenen Geräten verwalten. Außerdem können Sie sich aus der Ferne folgendermaßen abmelden:

1. Rufen Sie Bitdefender Central auf.
2. Klicken Sie auf das -Symbol in der rechten oberen Bildschirmecke.
3. Klicken Sie im Menü auf **Mein Konto**.
4. Öffnen Sie den Reiter **Sitzungsverwaltung**.
5. Wählen Sie im Bereich **Aktive Sitzungen** die Option **ABMELDEN** neben dem Gerät, für das Sie die Benutzersitzung beenden möchten.

## 3.4. Prüfen mit Bitdefender

### 3.4.1. Wie kann ich eine Datei oder einen Ordner scannen?

Um eine Datei oder einen Ordner einfach und schnell zu scannen, klicken Sie mit der rechten Maustaste auf das Objekt, das Sie scannen möchten, wählen Sie Bitdefender und anschließend **Mit Bitdefender scannen** aus dem Menü.

Um den Scan abzuschließen, folgen Sie den Anweisungen des Scan-Assistenten. Bitdefender wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen.

Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

Typische Situationen, für die diese Scan-Methode geeignet ist:

- Sie vermuten, dass eine bestimmte Datei oder ein Ordner infiziert ist.
- Immer dann, wenn Sie aus dem Internet Dateien herunterladen, von deren Ungefährlichkeit Sie nicht überzeugt sind.

- Scannen Sie einen freigegebenen Ordner, bevor Sie die enthaltenen Dateien auf Ihren Rechner kopieren.

## 3.4.2. Wie scanne ich mein System?

So können Sie einen vollständigen System-Scan durchführen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **VIRENSCHUTZ** auf **System-Scan**.
4. Folgen Sie den Anweisungen des Scan-Assistenten, um den Scan abzuschließen. Bitdefender wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen.

   Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen. Weitere Informationen finden Sie unter *„Viren-Scan-Assistent“* (S. 103).

## 3.4.3. Wie plane ich einen Scan?

Sie können Ihr Bitdefender-Produkt so konfigurieren, dass es wichtige Systembereiche nur dann scannt, wenn Sie Ihren Computer nicht benötigen.

So können Sie einen Scan planen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Scans verwalten**.
4. Wählen Sie den Scan-Typ aus, für den Sie einen Zeitplan festlegen möchten - Vollständiger System-Scan oder Quick Scan - und klicken Sie danach auf **Scan-Optionen**.

   Alternativ können Sie mit einem Klick auf **Neue benutzerdefinierte Aufgabe** einen eigenen Scan-Typ nach Ihren Anforderungen anlegen.
5. Aktivieren Sie den Schalter **Planen**.

   Wählen Sie eine der entsprechenden Optionen, um einen Zeitplan festzulegen:

- Start bei Systemneustart
- Einmal
- Periodisch

Im Fenster **Scan-Ziele** können Sie die Systembereiche festlegen, die gescannt werden sollen.

## 3.4.4. Wie kann ich eine benutzerdefinierte Scan-Aufgabe anlegen?

Wenn Sie bestimmte Bereiche Ihres Computers scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierte Scan-Aufgabe konfigurieren und ausführen.

Um eine benutzerdefinierte Scan-Aufgabe anzulegen, gehen Sie folgendermaßen vor:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Scans verwalten**.
4. Klicken Sie auf **Neue benutzerdefinierte Aufgabe**. Klicken Sie auf den Reiter **Basic**, um einen Namen für den Scan einzugeben und die Bereiche auszuwählen, die gescannt werden sollen.
5. Um die Scan-Optionen im Detail zu konfigurieren, wählen Sie den Reiter **Erweitert**.

   Sie können die Scan-Optionen einfach durch Einstellen der Scan-Tiefe festlegen. Schieben Sie den Regler dazu in die gewünschte Position.

   Sie können auch festlegen, dass der Computer heruntergefahren wird, wenn der Scan beendet und keine Bedrohung erkannt wurde. Bitte beachten Sie, dass dies das Standardverhalten bei jeder Ausführung dieser Aufgabe sein wird.
6. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.
7. Klicken Sie auf den entsprechenden Schalter, um einen Zeitplan für Ihre Scan-Aufgabe festzulegen.

8. Klicken Sie auf **Scan starten** und folgen Sie den Anweisungen des Scan-Assistenten, um den Scan abzuschließen. Wenn der Scan beendet wurde, werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.
9. Bei Bedarf können Sie einen bereits durchgeführten benutzerdefinierten Scan einfach erneut ausführen, indem Sie auf den entsprechenden Eintrag in der Liste klicken.

## 3.4.5. Wie kann ich einen Ordner vom Scan ausnehmen?

Mit Bitdefender können Sie bestimmte Dateien, Ordner oder Dateiendungen vom Scan ausschließen.

Ausschlüsse sollten nur von Benutzern eingesetzt werden, die erfahren im Umgang mit Computern sind und nur in den folgenden Situationen:

- Sie haben einen großen Ordner mit Filmen und Musik auf Ihrem System gespeichert.
- Sie haben ein großes Archiv mit verschiedenen Daten auf Ihrem System gespeichert.
- Sie haben einen Ordner, in dem Sie verschiedene Software-Typen und Anwendungen zu Testzwecken installieren. Ein Scan des Ordners könnte zum Verlust einiger der Daten führen.

So fügen Sie einen Ordner Ausschlussliste hinzu:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **VIRENSCHUTZ**.
4. Klicken Sie auf den Reiter **Ausschlüsse**.
5. Klicken Sie auf das Klappmenü **Vom Scan ausgeschlossene Dateien und Ordner** und danach auf **HINZUFÜGEN**.
6. Klicken Sie auf **Durchsuchen**, wählen Sie den Ordner aus, der von Scan ausgeschlossen werden soll, und wählen Sie danach den Scan-Typ aus, für den der Ausschluss gelten soll.

7. Klicken Sie auf **Hinzufügen**, um die Änderungen zu speichern und das Fenster zu schließen.

## 3.4.6. Wie gehe ich vor, wenn Bitdefender eine saubere Datei als infiziert eingestuft hat?

Es können Situationen auftreten, in denen Bitdefender einwandfreie Dateien irrtümlicherweise als Bedrohung einstuft (Fehlalarm). Um diesen Fehler zu korrigieren, fügen Sie die Datei der Bitdefender-Ausschlussliste hinzu:

1. Deaktivieren Sie den Bitdefender-Echtzeitvirenschutz:
   a. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
   b. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
   c. Klicken Sie auf das -Symbol unten rechts im Bereich **VIRENSCHUTZ**.
   d. Klicken Sie im Fenster **SCHILD** auf den AN/AUS-Schalter.

      Ein Warnung wird angezeigt. Sie müssen Ihre Auswahl bestätigen, indem Sie im Menü wählen, wie lange der Echtzeitschutz deaktiviert bleiben soll. Sie können den Echtzeitschutz für 5, 15 oder 30 Minuten, 1 Stunde, dauerhaft oder bis zum Neustart des Systems deaktivieren.
2. Lassen Sie sich die verborgenen Objekte in Windows anzeigen. Eine Anleitung hierzu finden Sie im Kapitel *„Wie kann ich in Windows versteckte Objekte anzeigen?“* (S. 87).
3. Stellen Sie die Datei aus der Quarantäne wieder her:
   a. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
   b. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
   c. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Quarantäne**.
   d. Wählen Sie die Datei aus und klicken Sie auf **WIEDERHERSTELLEN**.
4. Fügen Sie die Datei zur Ausschlussliste hinzu. Eine Anleitung hierzu finden Sie im Kapitel *„Wie kann ich einen Ordner vom Scan ausnehmen?“* (S. 65).
5. Aktivieren Sie den Bitdefender-Echtzeitvirenschutz.

6. Setzten Sie sich mit unseren Support-Mitarbeitern in Verbindung, damit wir die Erkennung des Updates der Bedrohungsinformationen entfernen können. Eine Anleitung hierzu finden Sie im Kapitel *„Hilfe anfordern“* (S. 341).

## 3.4.7. Wo sehe ich, welche Bedrohungen Bitdefender gefunden hat?

Nach jedem durchgeführten Scan wird ein Protokoll erstellt, in dem Bitdefender alle gefundenen Probleme aufzeichnet.

Der Bericht enthält detaillierte Informationen über den Scan-Vorgang, so wie Scan-Optionen, das Scan-Ziel, die gefundenen Bedrohungen und die Aktionen, die für diese Bedrohungen ausgeführt wurden.

Sobald der Scan beendet ist, können Sie das Scan-Protokoll direkt aus dem Scan-Assistenten heraus öffnen, indem Sie auf **PROTOKOLL ANZEIGEN** klicken.

So können Sie ein Scan-Protokoll oder gefundene Infektionen auch später anzeigen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wählen Sie unter dem Reiter **Alle** die Benachrichtigung bezüglich des neuesten Scans aus.

   Hier können Sie alle Ereignisse des Bedrohungs-Scans finden, einschließlich der Bedrohungen, die während Zugriff-Scans und vom Benutzer gestarteten Scans entdeckt wurden. Dazu kommen Statusänderungen für automatische Scans.
3. In der Benachrichtigungsliste können Sie überprüfen, welche Scans kürzlich durchgeführt wurden. Klicken Sie auf eine Benachrichtigung, um mehr darüber zu erfahren.
4. Um ein Scan-Protokoll zu öffnen, klicken Sie auf **PROTOKOLL ANZEIGEN**.

# 3.5. Elternberater

## 3.5.1. Wie kann ich meine Kinder vor Bedrohungen aus dem Internet schützen?

Der Bitdefender-Elternberater ermöglicht es, den Zugriff auf das Internet und bestimmte Applikationen zu beschränken. So verhindern Sie, dass sich Ihre Kinder unangemessene Inhalte ansehen, wenn Sie nicht anwesend sind.

So können Sie den Elternberater konfigurieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **ELTERNBERATER** auf **Konfigurieren**.

   Sie werden auf die Bitdefender-Konto Website weitergeleitet. Stellen Sie sicher, dass Sie sich mit Ihren Anmeldedaten angemeldet haben.
4. Das Dashboard für den Elternberater wird angezeigt. Hier können Sie die Einstellungen des Elternberaters einsehen und konfigurieren.
5. Klicken Sie rechts im Fenster **MEINE KINDER** auf **PROFIL HINZUFÜGEN**.
6. Geben Sie weitere Informationen wie Name und Geburtsdatum in die entsprechenden Felder ein. Um ein Profil-Foto hinzuzufügen, klicken Sie auf den Link **Datei auswählen**. Klicken Sie auf **NÄCHSTER SCHRITT**.

   Basierend auf Erkenntnissen zur Kindesentwicklung werden bei der Eingabe des Geburtsdatums des Kindes automatisch altersgerechte Einstellungen für die Internet-Suche voreingestellt.
7. Falls Bitdefender Total Security 2018 bereits auf dem Gerät Ihres Kindes installiert ist, wählen Sie dieses Gerät aus der entsprechenden Liste aus und dann das Konto, das Sie überwachen möchten. Klicken Sie auf **SPEICHERN**.

   Falls Ihr Kind ein Android- oder iOS-Gerät verwendet und der Bitdefender-Elternberater nicht installiert ist, klicken Sie auf **GERÄT HINZUFÜGEN**. Falls Ihr Kind ein Mac-Gerät verwendet und die App für Bitdefender Antivirus for Mac nicht installiert ist, klicken Sie auf die gleiche Schaltfläche. Wählen Sie das Betriebssystem aus, für das Sie die App

installieren möchten und klicken Sie auf **NÄCHSTER SCHRITT**, um fortzufahren.

8. Geben Sie die E-Mail-Adresse ein, an die wir den Download-Link für die Installation der Bitdefender-App senden sollen und klicken Sie anschließend auf **INSTALLATIONSLINK SENDEN**.

Über Bitdefender-Konto können Sie von jedem beliebigen Computer oder Mobilgerät mit Internetzugang aus die Online-Aktivitäten Ihrer Kinder überwachen und die Einstellungen des Elternberaters anpassen.

**Wichtig**

Auf Windows-basierten Geräten muss das Bitdefender Total Security 2018-Produkt, das in Ihrem Abonnement enthalten ist, heruntergeladen und installiert werden.

Auf macOS-Geräten muss das Bitdefender-Antivirus-for-Mac-Produkt heruntergeladen und installiert werden.

Auf Android- und iOS-Geräten muss die Anwendung für den Bitdefender-Elternberater heruntergeladen und installiert werden.

## 3.5.2. Wie hindere ich mein Kind daran, eine bestimmte Website aufzurufen?

Mit dem Bitdefender-Elternberater können Sie die Inhalte, die Ihr Kind auf seinem Gerät aufruft, steuern und den Zugriff auf bestimmte Websites blockieren.

Um den Zugriff auf eine Website zu blockieren, müssen Sie sie wie folgt zur Ausschlussliste hinzufügen:

1. Gehen Sie zu: https://central.bitdefender.com.
2. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Bitdefender-Konto an.
3. Klicken Sie auf **Elternberater**, um das Dashboard zu öffnen.
4. Wählen Sie im Fenster **MEINE KINDER** das Profil Ihres Kindes aus.
5. Klicken Sie auf den Reiter **Websites**.
6. Klicken Sie auf die Schaltfläche **VERWALTEN**.
7. Geben Sie die zu blockierende Website in das entsprechende Feld ein.
8. Wählen Sie **Zulassen** oder **Blockieren** aus.

9. Klicken Sie auf **Beenden**, um die Änderungen zu speichern.

> **Beachten Sie**
> Einschränkungen können nur für Android- und Windows-Geräte festgelegt werden.

## 3.5.3. Wie verhindere ich, dass mein Kind ein bestimmtes Spiel spielt?

Mit dem Bitdefender-Elternberater können Sie steuern, auf welche Inhalte Ihre Kinder auf dem Computer zugreifen können.

So können Sie den Zugriff auf ein Spiel blockieren:

1. Gehen Sie zu: https://central.bitdefender.com.
2. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Bitdefender-Konto an.
3. Klicken Sie auf **Elternberater**, um das Dashboard zu öffnen.
4. Wählen Sie im Fenster **MEINE KINDER** das Profil Ihres Kindes aus.
5. Klicken Sie auf den Reiter **Anwendungen**.

   Eine Liste mit Karten wird angezeigt. Die Karten zeigen die von Ihrem Kind verwendeten Apps.
6. Wählen Sie die Karte mit der App aus, die Ihr Kind nicht mehr verwenden soll.

   Ein Häkchen-Symbol zeigt an, dass Ihr Kind die App nicht mehr aufrufen kann.

## 3.5.4. Wie kann ich verhindern, dass mein Kind mit nicht vertrauenswürdigen Menschen in Kontakt kommt?

Mit dem Bitdefender-Elternberater können Sie Anrufe von unbekannten Telefonnummern oder von Freunden in der Kontaktliste Ihres Kindes blockieren.

So blockieren Sie einen bestimmten Kontakt auf einem Android-Gerät, auf dem der Bitdefender-Elternberater installiert ist:

1. Gehen Sie zu: https://central.bitdefender.com.

2. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Bitdefender-Konto an.
3. Klicken Sie auf **Elternberater**, um das Dashboard zu öffnen.
4. Wählen Sie das Profil des Kindes aus, für das Sie die Beschränkungen festlegen möchten.
5. Klicken Sie auf den Reiter **Telefonkontakte**.

   Eine Liste mit Karten wird angezeigt. Die Karten zeigen die Kontakte auf dem Telefon Ihres Kindes.
6. Wählen Sie die Karte mit der Telefonnummer aus, die Sie blockieren möchten.

   Ein Häkchen-Symbol zeigt an, dass Ihr Kind von der ausgewählten Nummer nicht mehr angerufen werden kann.

So blockieren Sie einen bestimmten Kontakt auf einem Android-Gerät, auf dem der Bitdefender-Elternberater nicht installiert ist:

1. Gehen Sie zu: https://central.bitdefender.com.
2. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Bitdefender-Konto an.
3. Klicken Sie auf **Elternberater**, um das Dashboard zu öffnen.
4. Wählen Sie das Profil des Kindes aus, für das Sie die Beschränkungen festlegen möchten.
5. Klicken Sie auf der gewünschten Karte auf **Elternberater auf einem Gerät installieren**.
6. Klicken Sie im angezeigten Fenster auf **GERÄT HINZUFÜGEN**.
7. Die Option **Bitdefender-Elternberater für Android** ist standardmäßig ausgewählt. Klicken Sie auf **NÄCHSTER SCHRITT** um fortzufahren, und installieren Sie dann die Anwendung auf den gewünschten Gerät.
8. Klicken Sie auf den Reiter **Telefonkontakte**.

   Eine Liste mit Karten wird angezeigt. Die Karten zeigen die Kontakte auf dem Android-Smartphone Ihres Kindes.
9. Wählen Sie die Karte mit der Telefonnummer aus, die Sie blockieren möchten.

Ein Häkchen-Symbol zeigt an, dass Ihr Kind von der ausgewählten Nummer nicht mehr angerufen werden kann.

Aktivieren Sie den Schalter **Unbekannte Nummern blockieren**, um unbekannte Telefonnummern zu blockieren.

**Beachten Sie**
Anrufeinschränkungen können nur für Android-Geräte festgelegt werden, die dem Profil Ihres Kindes hinzugefügt wurden.

## 3.5.5. Wie kann ich einen Ort als sichere oder unsichere Zone für mein Kind festlegen?

Mit dem Bitdefender-Elternberater können Sie sichere und unsichere Zonen für Ihr Kind festlegen.

So können Sie einen Aufenthaltsort festlegen:

1. Gehen Sie zu: https://central.bitdefender.com.
2. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Bitdefender-Konto an.
3. Klicken Sie auf **Elternberater**, um das Dashboard zu öffnen.
4. Wählen Sie im Fenster **MEINE KINDER** das Profil Ihres Kindes aus.
5. Klicken Sie auf den Reiter**Standort des Kindes**.
6. Im Fenster **Standort des Kindes** wird ein Rahmen angezeigt. Klicken Sie hier auf **Geräte**.
7. Klicken Sie auf **GERÄTE AUSWÄHLEN** und wählen Sie das zu konfigurierende Gerät aus.
8. Klicken Sie im Fenster **Zonen** auf die **ZONE HINZUFÜGEN**-Schaltfläche.
9. Wählen Sie aus, ob der Ort als **SICHER** oder **UNSICHER** gelten soll.
10. Geben Sie einen gültigen Namen für die Zone ein, die Ihr Kind aufsuchen bzw. nicht aufsuchen darf.
11. Legen Sie über den **Radius**-Regler einen Überwachungsradius fest.
12. Klicken Sie auf **ZONE HINZUFÜGEN**, um Ihre Einstellungen zu speichern.

Wenn Sie ein unsichere Zone als sichere Zone ausweisen möchten oder umgekehrt, klicken Sie sie an und klicken Sie danach auf die **ZONE**

**BEARBEITEN**. Wählen Sie je nach durchzuführender Änderung **SICHER** bzw. **UNSICHER** aus und klicken Sie danach auf **ZONE AKTUALISIEREN**.

## 3.5.6. Wie blockiere ich an Schultagen den Zugang meines Kindes zu den ausgewählten Geräten?

Mit dem Bitdefender-Elternberater können Sie den Zuganng Ihres Kindes zu den ausgewählten Geräten blockieren, wenn das Kind in der Schule ist oder Hausaufgaben machen soll.

So richten Sie die Einschränkungen ein:

1. Öffnen Sie den Bereich Elternberater in Bitdefender Central.
2. Wählen Sie im Fenster **MEINE KINDER** das Profil des Kindes, für das Sie Einschränkungen einrichten möchten.
3. Klicken Sie auf den Reiter **Zeitplan**.
4. Klicken Sie im Bereich **BEGRENZUNGEN TAGSÜBER** auf **KONKRET**.
5. Markieren Sie das Kästchen **Zeitbegrenzung Schultag**.
6. Wählen Sie im Raster die Zeitintervalle, in denen der Zugang blockiert werden soll.

**Beachten Sie**
Einschränkungen können nur für Android- und Windows-Geräte festgelegt werden.

## 3.5.7. Wie blockiere ich an Schultagen abends den Zugang meines Kindes zu den ausgewählten Geräten?

Mit dem Bitdefender-Elternberater können Sie den Zugang Ihres Kindes zu den ausgewählten Geräten an Schultagen auch abends einschränken.

So richten Sie die Einschränkungen ein:

1. Öffnen Sie den Bereich Elternberater in Bitdefender Central.
2. Wählen Sie im Fenster **MEINE KINDER** das Profil des Kindes, für das Sie Einschränkungen einrichten möchten.
3. Klicken Sie auf den Reiter **Zeitplan**.
4. Markieren Sie im Bereich **Abends/Nachts** das Kästchen **Schultag abends/nachts**.

5. Stellen Sie mit den Hoch- und Runter-Pfeilen die Intervalle ein, in denen der Zugang blockiert werden soll.

**Beachten Sie**
Einschränkungen können nur für Android- und Windows-Geräte festgelegt werden.

## 3.5.8. Wie blockiere ich am Wochenende den Zugang meines Kindes zu den ausgewählten Geräten?

Mit dem Bitdefender-Elternberater können Sie den Zugang Ihres Kindes zu den ausgewählten Geräten an Wochenenden einschränken.

So richten Sie die Einschränkungen ein:

1. Öffnen Sie den Bereich Elternberater in Bitdefender Central.
2. Wählen Sie im Fenster **MEINE KINDER** das Profil des Kindes, für das Sie Einschränkungen einrichten möchten.
3. Klicken Sie auf den Reiter **Zeitplan**.
4. Markieren Sie im Bereich **ABENDS/NACHTS** das Kästchen **Wochenende abends/nachts**.
5. Stellen Sie mit den Hoch- und Runter-Pfeilen die Intervalle ein, in denen der Zugang blockiert werden soll.
6. Im Bereich**BEGRENZUNGEN TAGSÜBER** haben Sie folgende Optionen:

   - **KUMULATIV**
     a. Markieren Sie das Kästchen **Zeitbegrenzung Wochenende**.
     b. Stellen Sie mithilfe der Schieber ein, für wie lange der Zugang erlaubt ist.
   - **KONKRET**
     a. Markieren Sie das Kästchen **Zeitbegrenzung Wochenende**.
     b. Wählen Sie im Raster die Zeitintervalle, in denen der Zugang blockiert werden soll.

   Bitte beachten Sie, dass die Einstellungen **KUMULATIV** und **KONKRET** nicht miteinander funktionieren.

**Beachten Sie**
Einschränkungen können nur für Android- und Windows-Geräte festgelegt werden.

### 3.5.9. Wie entferne ich das Profil für mein Kind?

So können Sie ein bestehendes Profil für ein Kind entfernen:

1. Gehen Sie zu: https://central.bitdefender.com.
2. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Bitdefender-Konto an.
3. Klicken Sie auf **Elternberater**, um das Dashboard zu öffnen.
4. Klicken Sie in dem Profil, das Sie löschen möchten, auf das -Symbol und wählen Sie **Entfernen**.

## 3.6. Privatshpäreschutz

### 3.6.1. Wie sichere ich meine Online-Transaktionen ab?

Um Ihre Online-Transaktionen wie Online-Banking noch sicherer zu machen, können Sie den Browser von Bitdefender verwenden.

Bitdefender Safepay™ ist ein abgesicherter Browser, der Ihre Kreditkartennummern, Kontonummern und andere sensible Daten, die Sie bei Online-Transaktionen eingeben, zuverlässig schützt.

So können Sie Ihre Online-Aktivitäten absichern und vor neugierigen Augen schützen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf die **Safepay**-Schaltfläche.
3. Klicken Sie auf die Schaltfläche , um die **Virtuelle Tastatur** aufzurufen.

   Verwenden Sie die **Virtuelle Tastatur** immer dann, wenn Sie sensible Informationen wie Passwörter eingeben.

## 3.6.2. Was kann ich tun, wenn mein Gerät gestohlen wurde?

Der Diebstahl von Mobilgeräten, egal ob Smartphone, Tablet oder Laptop, ist heute ein weit verbreitetes Problem, von dem Privatpersonen und Unternehmen in der ganzen Welt betroffen sind.

Mit dem Bitdefender-Diebstahlschutz können Sie das gestohlene Gerät nicht nur orten und verriegeln, sondern im Notfall auch sämtliche Daten von der Festplatte löschen, damit Sie dem Dieb nicht in die Hände fallen.

So können Sie über Ihr Benutzerkonto auf die Diebstahlschutzfunktionen zugreifen:

1. Rufen Sie Bitdefender Central auf.
2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie auf die entsprechende Gerätekarte und wählen Sie **Diebstahlschutz** aus.
4. Wählen Sie die Funktion, die Sie verwenden möchten:
   - **ORTEN** - Zeigt den Standort Ihres Geräts auf Google Maps an.
   - **Benachrichtigung** - Schickt eine Benachrichtigung auf das Gerät.
   - **Verriegeln** - den Computer verriegeln und eine numerische PIN zur Entriegelung festlegen. Alternativ können Sie die entsprechende Option aktivieren, um Bitdefender zu erlauben, Fotos von Personen aufzunehmen, die auf Ihr Gerät zugreifen wollen.
   - **Löschen** - sämtliche Daten vom Computer löschen.

     **Wichtig**
     Nach einer Löschung funktionieren die Diebstahlschutz-Funktionen nicht mehr.

   - **IP anzeigen** - Zeigt die letzte IP-Adresse für das ausgewählte Gerät an.

## 3.6.3. Wie benutze ich einen Datentresor?

Der Bitdefender-Datentresor bietet Ihnen die Möglichkeit, verschlüsselte, passwortgeschützte logische Laufwerke (oder Datentresore) auf Ihrem Computer zu erstellen, in denen Sie Ihre wichtigen und vertraulichen Daten sicher speichern können. Physisch gesehen ist der Tresor eine auf der lokalen Festplatte gespeicherte Datei mit der Endung .bvd.

Wenn Sie einen Datentresor erstellen, sind zwei Aspekte wichtig: die Größe und das Passwort. Die voreingestellte Größe von 100 MB sollte für Ihre privaten Dokumente, Exel-Dateien und andere Daten ausreichen. Für Videos und andere große Dateien jedoch benötigen Sie mehr Speicherplatz.

So können Sie Ihre vertraulichen Dateien und Ordner sicher in einem Bitdefender-Datentresor speichern:

- **Erstellen Sie einen Datentresor und vergeben Sie ein sicheres Passwort dafür.**

  Um einen Tresor zu erstellen, klicken Sie mit der rechten Maustaste auf einen leeren Bereich auf dem Desktop oder in einem Ordner auf Ihrem Computer, wählen Sie **Bitdefender** > **Bitdefender -Datentresor** und anschließend **Tresor erstellen**.

  Ein neues Fenster wird angezeigt. Gehen Sie wie folgt vor:

  1. Klicken Sie auf **Durchsuchen**, wählen Sie den gewünschten Speicherort und speichern Sie die Tresordatei unter dem gewünschten Namen.
  2. Wählen Sie einen Laufwerkbuchsbuchstaben aus dem Menü. Wenn Sie einen Datentresor öffnen, wird ein virtuelles Laufwerk mit dem gewählten Laufwerksbuchstaben unter **Arbeitsplatz** erscheinen.
  3. Geben Sie das Datentresorpasswort im Feld **Passwort** ein und bestätigen Sie dieses im dem Feld **Bestätigen**.
  4. Sie können die Standardgröße (100 MB) des Datentresors über die Pfeiltasten im Drehfeld **Tresorgröße (MD)** ändern.
  5. Klicken Sie auf **Erstellen**.

  > **Beachten Sie**
  > Wenn Sie einen Datentresor öffnen, erscheint ein virtuelles Laufwerk unter **Arbeitsplatz**. Dieses Laufwerk hat den Laufwerksbuchstaben, der dem Datentresor zugewiesen wurde.

- **Dateien oder Verzeichnisse, die Sie sichern möchten, dem Tresor hinzufügen.**

  Um eine Datei in einem Tresor zu speichern, müssen Sie den entsprechenden Tresor zuerst öffnen.

  1. Blättern Sie zur entsprechenden .bvd-Tresordatei.

2. Rechtsklicken Sie auf die Tresordatei, bewegen Sie den Mauszeiger auf Bitdefender-Tresordatei und wählen Sie **Öffnen**.
3. Ein neues Fenster wird angezeigt. Geben Sie das Passwort ein, wählen Sie einen Laufwerkbuchstaben aus, der dem Tresor zugeordnet werden soll, und klicken Sie auf **OK**.

Sie können nun in dem Laufwerk, in dem der entsprechende Datentresor gespeichert ist, wie gewohnt Windows-Explorer-Operationen durchführen. Um einem offenen Datentresor eine Datei hinzuzufügen, rechtsklicken Sie auf die Datei, bewegen Sie den Mauszeiger auf den Bitdefender-Datentresor und wählen Sie **Dem Datentresor hinzufügen**.

- **Der Tresor sollte jederzeit geschlossen sein.**

  Öffnen Sie einen Tresor nur, wenn Sie auf eine der Dateien zugreifen oder dessen Inhalt verwalten möchten. Um einen Tresor zu verriegeln, klicken Sie mit der rechten Maustaste unter **Arbeitsplatz** auf den entsprechenden Tresor, bewegen Sie den Mauszeiger auf **Bitdefender-Datentresor** und wählen Sie **Verriegeln**.

- **Stellen Sie sicher, dass Sie die Tresordatei .bvd nicht löschen.**

  Durch das Löschen der Datei werden auch die Tresorinhalte gelöscht.

Weitere Informationen zur Handhabung von Datentresoren finden Sie im Kapitel *„Verschlüsselung“* (S. 148).

## 3.6.4. Wie lösche ich mit Bitdefender eine Datei unwiderruflich?

Wenn Sie eine Datei unwiderruflich von Ihrem System löschen möchten, müssen Sie die Datei physisch von Ihrer Festplatte entfernen.

Mit dem Bitdefender-Dateischredder können Sie über das Windows-Kontextmenü Dateien oder Ordner auf Ihrem Computer schnell und einfach schreddern. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner, den Sie unwiderruflich löschen möchten, wählen Sie Bitdefender und anschließend **Dateischredder**.
2. Ein Bestätigungsfenster wird angezeigt. Klicken Sie auf **JA, LÖSCHENa**, um den Assistenten für den Dateischredder zu starten.

Bitte warten Sie, bis Bitdefender das Schreddern der Dateien abgeschlossen hat.

3. Die Ergebnisse werden angezeigt. Klicken Sie auf **BEENDEN** um den Assistenten zu schließen.

### 3.6.5. Wie schütze ich meine Webcam vor Hackern?

So können Sie Ihr Bitdefender so konfigurieren, dass es den Zugriff installierter Anwendungen auf Ihre Webcam zulässt oder verweigert:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **WEBCAM-SCHUTZ** auf **Webcam-Zugriff**.

   Es wird eine Liste mit Apps angezeigt, die den Zugriff auf Ihre Kamera angefordert haben.
4. Bewegen Sie den Mauszeiger auf die Anwendung, deren Zugriff Sie zulassen oder verweigern möchten, und klicken Sie danach auf den entsprechenden Schalter.

   Klicken Sie auf das -Symbol, um anzuzeigen, welche Auswahl andere Bitdefender-Benutzer für die ausgewählte App getroffen haben. Sie werden unabhängig von der Autopilot-Einstellung benachrichtigt, sobald eine der Apps in der Liste von den Bitdefender-Benutzern blockiert wurde.

Klicken Sie auf den Link **Eine neue Anwendung zur Liste hinzufügen**, um Apps manuell zu der Liste hinzuzufügen.

## 3.7. Optimierungstools

### 3.7.1. Wie verbessere ich die Leistung meines Systems?

Die Systemleistung hängt nicht allein von der Hardware-Konfiguration wie Prozessorauslastung, Speichernutzung und Festplattenspeicher ab. Sie hängt zudem auch direkt von Ihrer Systemkonfiguration und Datenverwaltung ab.

Dies sind die Hauptaktionen, die Sie mit Bitdefender durchführen können, um die Systemgeschwindigkeit und -leistung zu verbessern.

- *„Optimieren Sie Ihre Systemgeschwindigkeit mit nur einem Klick“* (S. 80)
- *„Scannen Sie Ihr System regelmäßig“* (S. 80)


## Optimieren Sie Ihre Systemgeschwindigkeit mit nur einem Klick

Mit der Ein-Klick-Optimierung sparen Sie wertvolle Zeit bei der Verbesserung Ihrer Systemleistung, indem nicht mehr benötigte Dateien innerhalb kürzester Zeit gescannt, erkannt und bereinigt werden.

So können Sie den Prozess für die Ein-Klick-Optimierung starten:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf die Schaltfläche **Ein-Klick-Optimierung**.
3. Lassen Sie Bitdefender nach Dateien suchen, die gelöscht werden können, und klicken Sie auf **OPTIMIEREN**, um den Vorgang abzuschließen.

Weitere Informationen, wie Sie die Systemgeschwindigkeit mit nur einem Klick verbessern können, erhalten Sie in Kapitel *„Optimierung der Systemgeschwindigkeit mit nur einem Klick“* (S. 188).

## Scannen Sie Ihr System regelmäßig

Die Geschwindigkeit und das allgemeine Verhalten Ihres Systems kann auch durch Bedrohungen beeinträchtigt werden.

Stellen Sie sicher, dass Ihr System regelmäßig gescannt wird, mindestens einmal pro Woche.

Es empfiehlt sich, einen System-Scan durchzuführen, da so nach allen Bedrohungen gesucht wird, die die Sicherheit Ihres Systems gefährden. Darüber hinaus werden auch die Inhalte von Archiven gescannt.

So können Sie einen System-Scan starten:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **VIRENSCHUTZ** auf **System-Scan**.
4. Befolgen Sie die Anweisungen des Assistenten.

### 3.7.2. Wie kann ich meine Systemstartzeit verbessern?

Nicht benötigte Anwendungen, die lästigerweise den Start des Systems verlangsamen, können mit der Systemstartoptimierung deaktiviert oder ihr Start verschoben werden, was Ihnen wertvolle Zeit spart.

So verwenden Sie die Systemstartoptimierung:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf die Schaltfläche **Systemstartoptimierung**.
3. Wählen Sie die Anwendungen aus, die Sie beim Systemstart verzögern möchten.

Weitere Informationen, wie Sie die Startzeit Ihres PCs optimieren können, finden Sie in Kapitel *„Optimieren der Systemstartzeit“* (S. 189).

## 3.8. Nützliche Informationen

### 3.8.1. Wie kann ich meine Sicherheitslösung selbst testen?

Um die ordnungsgemäße Funktion Ihres Bitdefender-Produkts zu überprüfen, empfehlen wir den EICAR-Test.

Dabei testen Sie mithilfe der speziell für diesen Zweck entwickelten EICAR-Testdatei Ihre Sicherheitslösung.

Gehen Sie folgendermaßen vor, um Ihre Sicherheitslösung zu testen:

1. Laden Sie die Testdatei von der offiziellen EICAR-Website unter http://www.eicar.org/ herunter.
2. Klicken Sie auf den Reiter **Anti-Malware Testfile**.
3. Klicken Sie im Menü links auf **Download**.
4. Klicken Sie unter **Download area using the standard protocol http** auf die **eicar.com**-Testdatei.
5. Sie werden informiert, dass die von Ihnen aufgerufene Seite die EICAR-Testdatei (keine Bedrohung) enthält.

   Wenn Sie auf **Ich bin mir der Risiken bewusst und möchte trotzdem fortfahren** klicken, beginnt der Download der Testdatei und ein Bitdefender-Fenster informiert Sie, dass eine Bedrohung erkannt wurde.

Klicken Sie auf **Mehr...** für weitere Informationen.

Falls Sie keine Bitdefender-Benachrichtigung erhalten, empfehlen wir Ihnen, sich wie in Kapitel *„Hilfe anfordern“ (S. 341)* beschrieben an Bitdefender zu wenden.

## 3.8.2. Wie kann ich Bitdefender entfernen?

So können Sie Ihr Bitdefender Total Security 2018 entfernen:

- In **Windows 7**:
  1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
  2. Suchen Sie **Bitdefender Total Security 2018** und wählen Sie **Deinstallieren**.
  3. Klicken Sie im angezeigten Fenster auf **Entfernen**.
  4. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.
- In **Windows 8 und Windows 8.1**:
  1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
  2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
  3. Suchen Sie **Bitdefender Total Security 2018** und wählen Sie **Deinstallieren**.
  4. Klicken Sie im angezeigten Fenster auf **Entfernen**.
  5. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.
- In **Windows 10**:
  1. Klicken Sie auf **Start** und danach auf Einstellungen.
  2. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie danach auf **Installierte Anwendungen**.
  3. Suchen Sie **Bitdefender Total Security 2018** und wählen Sie **Deinstallieren**.
  4. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.

5. Klicken Sie im angezeigten Fenster auf **Entfernen**.
6. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.

**Beachten Sie**
Wenn Sie bei der Neuinstallation so vorgehen, werden die benutzerdefinierten Einstellungen endgültig gelöscht.

## 3.8.3. Wie kann ich Bitdefender VPN entfernen?

Bei der Entfernung von Bitdefender VPN gehen Sie ganz ähnlich vor, wie bei der Entfernung anderer Programme:

- In **Windows 7**:
  1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
  2. Suchen Sie **Bitdefender VPN** und klicken Sie auf **Deinstallieren**.

     Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist.
- In **Windows 8 und Windows 8.1**:
  1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
  2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
  3. Suchen Sie **Bitdefender VPN** und klicken Sie auf **Deinstallieren**.

     Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist.
- In **Windows 10**:
  1. Klicken Sie auf **Start** und danach auf Einstellungen.
  2. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie danach auf **Installierte Anwendungen**.
  3. Suchen Sie **Bitdefender VPN** und klicken Sie auf **Deinstallieren**.
  4. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.

     Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist.

## 3.8.4. Wie fahre ich den Computer automatisch herunter, nachdem der Scan beendet wurde?

Bitdefender bietet unterschiedliche Scan-Aufgaben, mithilfe derer Sie sicherstellen können, dass Ihr System nicht durch Bedrohungen infiziert wurde. Je nach Software- und Hardwarekonfiguration kann ein Scan des gesamten Systems längere Zeit in Anspruch nehmen.

Deshalb können Sie Bitdefender so konfigurieren, dass Ihr Produkt den Computer herunterfährt, sobald der Scan abgeschlossen ist.

Stellen Sie sich folgende Situation vor: Sie sind mit der Arbeit an Ihrem Computer fertig und möchten ins Bett gehen. Sie möchten aber nun noch Ihr System durch Bitdefender auf Bedrohungen prüfen lassen.

So können Sie einstellen, dass Bitdefender den Computer herunterfährt, sobald der Scan abgeschlossen ist:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Scans verwalten**.
4. Klicken Sie im Fenster **SCAN-AUFGABEN VERWALTEN** auf **Neue benutzerdefinierte Aufgabe**, um einen Namen für den Scan einzugeben und die Bereiche auszuwählen, die gescannt werden sollen.
5. Um die Scan-Optionen im Detail zu konfigurieren, wählen Sie den Reiter **Erweitert**.
6. Markieren Sie die Option, dass der Computer heruntergefahren wird, wenn der Scan beendet und keine Bedrohung gefunden wurde.
7. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.
8. Klicken Sie auf **Scan starten**, um Ihr System zu scannen.

Wenn keine Bedrohungen gefunden wurden, wird der Computer heruntergefahren.

Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen. Weitere Informationen finden Sie unter *„Viren-Scan-Assistent“* (S. 103).

## 3.8.5. Wie konfiguriere ich Bitdefender für die Nutzung einer Proxy-Verbindung?

Wenn Ihr Computer sich über einen Proxy-Server mit dem Internet verbindet, müssen Sie Bitdefender mit den Proxy-Einstellungen konfigurieren. Normalerweise findet und importiert Bitdefender automatisch die Proxy-Einstellungen Ihres Systems.

**Wichtig**
Internet-Verbindungen in Privathaushalten nutzen üblicherweise keine Proxy-Server. Als Faustregel gilt, dass Sie die Einstellungen der Proxy-Verbindung Ihrer Bitdefender-Anwendung prüfen und konfigurieren sollten, falls Updates nicht funktionieren. Wenn Bitdefender sich aktualisieren kann, dann ist es richtig konfiguriert, um eine Verbindung mit dem Internet aufzubauen.

So können Sie Ihre Proxy-Einstellungen verwalten:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das ⚙-Symbol.
2. Wechseln Sie zum Reiter **ERWEITERT**.
3. Aktivieren Sie die Proxy-Nutzung, indem Sie auf den entsprechenden Schalter klicken.
4. Klicken Sie auf den Link **Proxyverwaltung**
5. Sie haben zwei Möglichkeiten, die Proxy-Einstellungen vorzunehmen:
   - **Proxy-Einstellungen aus Standard-Browser importieren** - Proxy-Einstellungen des aktuellen Benutzers, aus dem Standard-Browser importiert. Sollte ein Benutzername und Passwort nötig sein so geben Sie diesen in die dafür vorgesehenen Felder ein.

     **Beachten Sie**
     Bitdefender kann die Proxy-Einstellungen aus den gängigsten Browsern importieren, einschließlich der neuesten Versionen von Internet Explorer, Mozilla Firefox und Google Chrome.

   - **Benutzerdefinierte Proxy-Einstellungen** - Proxy-Einstellungen, die Sie selbst konfigurieren können. Die folgenden Einstellungen müssen angegeben werden:

- **Adresse** - Geben Sie die IP-Adresse des Proxy-Servers ein.
- **Port** - Geben Sie den Port ein, über den Bitdefender die Verbindung zum Proxy-Server herstellt.
- **Name** - Geben Sie einen für den Proxy-Server gültigen Benutzernamen ein.
- **Passwort** - Geben Sie das Passwort für den zuvor angegebenen Benutzer ein.

6. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Bitdefender wird die verfügbaren Proxy-Einstellungen verwenden, bis die Lösung eine Verbindung mit dem Internet aufbauen kann.

## 3.8.6. Ist auf meinem System die 32- oder 64-Bit-Version von Windows installiert?

So können Sie ermitteln, ob Sie über ein 32-Bit- oder 64-Bit-Betriebssystem verfügen:

- In **Windows 7**:
  1. Klicken Sie auf **Start**.
  2. Finden Sie **Computer** im **Start**-Menü.
  3. Rechtsklicken Sie auf **Arbeitsplatz** und wählen Sie **Eigenschaften**.
  4. Unter **System** können Sie die Systeminformationen einsehen.
- In **Windows 8**:
  1. Finden Sie auf der Windows-Startseite den Eintrag **Computer** (z.B. durch die Eingabe von "Computer" auf der Startseite) und klicken Sie auf das entsprechende Symbol.

     Finden Sie unter **Windows 8.1 Dieser PC**.
  2. Wählen Sie im Menü unten **Eigenschaften**.
  3. Im Bereich System finden Sie Ihren Systemtyp.
- In **Windows 10**:
  1. Geben Sie "System" in das Suchfeld in der Taskleiste ein und klicken Sie auf das entsprechende Symbol.
  2. Im Bereich System finden Sie Informationen zu Ihrem Systemtyp.

## 3.8.7. Wie kann ich in Windows versteckte Objekte anzeigen?

Diese Schritte sind sinnvoll in den Fällen, in denen Sie es mit einer Bedrohungssituation zu tun haben und Sie infizierte Dateien, die eventuell verborgen sind, finden und entfernen müssen.

Gehen Sie folgendermaßen vor, um versteckte Objekte in Windows anzuzeigen:

1. Klicken Sie auf **Start** und öffnen Sie die **Systemsteuerung**.

   In **Windows 8 und Windows 8.1**: Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.

2. Klicken Sie auf **Ordneroptionen**.
3. Gehen Sie auf den Reiter **Ansicht**.
4. Wählen Sie **Verborgene Dateien und Verzeichnisse anzeigen**.
5. Entfernen Sie den Haken bei **Erweiterungen bei bekannten Dateitypen ausblenden**.
6. Deaktivieren Sie **Geschützte Betriebssystemdateien verbergen**.
7. Klicken Sie auf **Anwenden** und danach auf **OK**.

In **Windows 10**:

1. Geben Sie "Alle Dateien und Ordner anzeigen" in das Suchfeld in der Taskleiste ein und klicken Sie auf das entsprechende Symbol.
2. Wählen Sie **Ausgeblendete Dateien, Ordner und Laufwerke anzeigen** aus.
3. Entfernen Sie den Haken bei **Erweiterungen bei bekannten Dateitypen ausblenden**.
4. Deaktivieren Sie **Geschützte Betriebssystemdateien verbergen**.
5. Klicken Sie auf **Anwenden** und danach auf **OK**.

## 3.8.8. Wie entferne ich andere Sicherheitslösungen?

Der Hauptgrund für den Einsatz einer Sicherheitslösung ist der Schutz und die Sicherheit Ihrer Daten. Aber was geschieht, wenn mehr als ein Sicherheitsprogramm auf demselben System läuft?

Wenn Sie mehr als eine Sicherheitslösung auf Ihrem Computer verwenden, wird dadurch das System instabil. Das Bitdefender Total Security 2018-Installationsprogramm findet automatisch andere auf dem System installierte Sicherheits-Software und bietet an, diese zu deinstallieren.

Falls Sie weitere bereits auf dem PC installierte Sicherheitslösungen nicht während der Installation entfernt haben:

- In **Windows 7**:
  1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
  2. Warten Sie einen Moment, bis die Liste der installierten Software angezeigt wird.
  3. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.
  4. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.
- In **Windows 8 und Windows 8.1**:
  1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
  2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
  3. Warten Sie einen Moment, bis die Liste der installierten Software angezeigt wird.
  4. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.
  5. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.
- In **Windows 10**:
  1. Klicken Sie auf **Start** und danach auf Einstellungen.
  2. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie danach auf **Installierte Anwendungen**.
  3. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.
  4. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.

5. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.

Wenn es Ihnen nicht gelingt, weitere auf Ihrem Rechner installierte Sicherheits-Software zu entfernen, laden Sie sich das Deinstallations-Tool von der Website des entsprechenden Herstellers herunter oder wenden Sie sich direkt an den Hersteller für eine Deinstallationsanleitung.

## 3.8.9. Wie führe ich einen Neustart im abgesicherten Modus durch?

Der abgesicherte Modus ist ein diagnostischer Betriebsmodus, der hauptsächlich bei der Suche nach Fehlern zum Einsatz kommt, die den normalen Windows-Betrieb beeinträchtigen. Solche Probleme reichen von in Konflikt stehenden Treibern bis hin zu Bedrohungen, die Windows daran hindern, normal hochzufahren. Im abgesicherten Modus funktionieren nur einige wenige Anwendungen und Windows lädt nur die wichtigsten Treiber und ein Minimum an Betriebssystemkomponenten. Deshalb sind bei einer Verwendung von Windows im abgesicherten Modus die meisten Bedrohungen inaktiv und können einfach entfernt werden.

Start von Windows im abgesicherten Modus:

- In **Windows 7**:
  1. Starten Sie Ihren Computer neu.
  2. Drücken Sie wiederholt die **F8**-Taste, bevor Windows startet, um so Zugriff auf das Boot-Menü zu erhalten.
  3. Wählen Sie **Abgesicherter Modus** im Boot-Menü oder **Abgesicherter Modus mit Netzwerktreibern**, falls Sie Zugang zum Internet haben möchten.
  4. Drücken Sie die **Eingabetaste** und warten Sie, während Windows im abgesicherten Modus startet.
  5. Dieser Vorgang endet mit einer Bestätigungsbenachrichtigung. Klicken Sie zur Bestätigung auf **OK**.
  6. Um Windows normal zu starten, starten Sie einfach Ihr System neu.
- In **Windows 8, Windows 8.1 und Windows 10**:
  1. Rufen Sie die **Systemkonfiguration** in Windows auf, indem Sie auf Ihrer Tastatur gleichzeitig die Tasten **Windows + R** drücken.

2. Geben Sie **msconfig** in das **Öffnen**-Dialogfeld ein und klicken Sie auf **OK**.
3. Wechseln Sie zum Reiter **Boot**.
4. Aktivieren Sie im Bereich **Startoptionen** das Kästchen **Sicherer Start**.
5. Klicken Sie auf **Netzwerk** und dann auf **OK**.
6. Im Fenster **Systemkonfiguration** werden Sie darüber informiert, dass Ihr System zur Übernahme der Änderungen neu gestartet werden muss. Klicken Sie auf **OK**.

   Ihr System wird im Abgesicherten Modus mit Netzwerktreibern neu gestartet.

Setzen Sie die Einstellungen zurück, um Ihr System im Normalen Modus neu zu starten. Starten Sie dazu den **Systemvorgang** erneut und deaktivieren Sie das Kästchen **Sicherer Start**. Klicken Sie auf **OK** und dann auf **Neustart**. Warten Sie, bis die neuen Einstellungen übernommen wurden.

# 4. DIE SICHERHEITSELEMENTE IM DETAIL

## 4.1. Virenschutz

Bitdefender schützt Sie vor allen Arten von Bedrohungen (Malware, Trojaner, Spyware, Rootkits etc.). Der Virenschutz, den Bitdefender bietet, lässt sich in zwei Kategorien einteilen:

- Zugriff-Scan - Verhindert, dass neue Bedrohungen auf Ihr System gelangen. Bitdefender wird z.B. ein Worddokument auf Malware scannen, wenn Sie es öffnen oder eine Email-Nachricht, wenn Sie diese empfangen.

  Der Zugriff-Scan stellt den Echtzeitschutz vor Bedrohungen sicher und ist damit ein grundlegender Bestandteil jedes Computer-Sicherheitsprogramms.

  > **Wichtig**
  > Um zu verhindern, dass Ihr Computer durch Bedrohungen infiziert wird, sollte der **Zugriff-Scan** immer aktiviert bleiben.

- On-demand Prüfung - erkennt und entfernt die Bedrohung, die sich bereits auf dem System befindet. Hierbei handelt es sich um einen klassischen, durch den Benutzer gestarteten, Scan - Sie wählen das Laufwerk, Verzeichnis oder Datei, die Bitdefender scannen soll und Bitdefender scannt diese.

Bitdefender scannt automatisch alle Wechselmedien, die mit dem Computer verbunden sind, um einen sicheren Zugriff zu garantieren. Weitere Informationen finden Sie unter *„Automatischer Scan von Wechselmedien“* (S. 107).

Erfahrene Benutzer können Scan-Ausschlüsse konfigurieren, wenn Sie nicht möchten, dass bestimmte Dateien oder Dateitypen gescannt werden. Weitere Informationen finden Sie unter *„Konfiguration der Scan-Ausschlüsse“* (S. 110).

Wenn Bitdefender eine Bedrohung erkennt, versucht das Programm automatisch den Schad-Code der infizierten Datei zu entfernen und die Originaldatei wiederherzustellen. Diese Operation bezeichnet man als Desinfektion. Dateien, die nicht desinfiziert werden können, werden in die Quarantäne verschoben, um so die Infizierung einzudämmen. Weitere Informationen finden Sie unter *„Verwalten von Dateien in Quarantäne“* (S. 113).

Wenn Ihr Computer durch Bedrohungen infiziert wurde, siehe *„Entfernung von Bedrohungen“* (S. 223). Um Ihnen bei der Entfernung von Bedrohungen zu helfen, die nicht von innerhalb des Windows-Betriebssystems entfernt werden können, stellt Bitdefender Ihnen einen*„Bitdefender-Rettungsmodus (Rettungsumgebung unter Windows 10)“* (S. 224). Dabei handelt es sich um eine vertrauenswürdige Umgebung, die speziell der Entfernung von Bedrohungen dient und es Ihnen ermöglicht, Ihren Computer unabhängig von Windows zu starten. Wenn der Computer im Rettungsmodus (Rettungsumgebung unter Windows 10) läuft, sind Windows-Bedrohungen inaktiv, wodurch sie sich leicht entfernen lassen.

### 4.1.1. Zugriff-Scans (Echtzeitschutz)

Bitdefender bietet durch die Prüfung aller aufgerufenen Dateien und E-Mail-Nachrichten durchgehenden Echtzeitschutz vor einer Vielzahl von Bedrohungen.

#### Aktivieren / Deaktivieren des Echtzeitschutzes

So können Sie den Echtzeitschutz vor Bedrohungen aktivieren oder deaktivieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **VIRENSCHUTZ**.
4. Klicken Sie im Fenster **SCHILD** auf den AN/AUS-Schalter.
5. Wenn Sie den Echtzeitschutz deaktivieren, wird ein Warnfenster angezeigt. Sie müssen Ihre Auswahl bestätigen, indem Sie im Menü wählen, wie lange der Echtzeitschutz deaktiviert bleiben soll. Sie können den Echtzeitschutz für 5, 15 oder 30 Minuten, 1 Stunde, dauerhaft oder bis zum Neustart des Systems deaktivieren. Der Echtzeitschutz wird automatisch nach Ablauf des festgelegten Zeitraums aktiviert.

**Warnung**
Hierbei handelt es sich um ein grobes Sicherheitsrisiko. Wir empfehlen den Echtzeitschutz so kurz wie möglich zu deaktivieren. Während der Echtzeitschutz deaktiviert ist, sind Sie nicht vor Bedrohungen geschützt.

## Erweiterte Einstellungen des Echtzeitschutzes konfigurieren

Erfahrene Benutzer können die Scan-Einstellungen von Bitdefender nutzen. Sie können die Einstellungen für den Echtzeitschutz im Detail konfigurieren, indem Sie eine benutzerdefinierte Sicherheitsstufe festlegen.

So können Sie die erweiterten Einstellungen für den Echtzeitschutz konfigurieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **VIRENSCHUTZ**.
4. Klicken Sie im Fenster **SCHILD** auf das Akkordeonmenü **ERWEITERTE EINSTELLUNGEN ANZEIGEN**.

   Ein unterteiltes Fenster wird angezeigt.
5. Scrollen Sie nach unten, um die Scan-Einstellungen wie benötigt festzulegen.

## Informationen zu den Scan-Optionen

Diese Informationen sind vielleicht nützlich:

- Wenn Ihnen bestimmte Begriffe nicht geläufig sind, schlagen Sie diese im Glossar nach. Sie könne auch durch eine Suche im Internet hilfreiche Informationen finden.
- **Scan-Optionen für aufgerufene Dateien.** Sie können Bitdefender so einstellen, dass Dateien oder Anwendungen (Programmdateien) nur bei Zugriff gescannt werden. Das Scannen aller Dateien bietet den besten Schutz, während das ausschließliche Scannen der Anwendungen nur für die Verbesserung der Systemleistung verwendet werden kann.

  Standardmäßig werden sowohl lokale Ordner als auch Netzwerkfreigaben durch Zugriff-Scans gescannt. Wenn Sie Ihre Systemleistung erhöhen möchten, können Sie Netzwerk-Ordner von Zugriff-Scans ausschließen.

  Anwendungen (oder Programmdateien) sind weitaus anfälliger für Angriffe durch Bedrohungen als andere Dateitypen. Diese Kategorie beinhaltet die folgenden Dateierweiterungen:

386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Inhalt von Archiven scannen.** Das Scannen von Archiven ist ein langsamer und ressourcen-intensiver Vorgang, der aus diesem Grund nicht für den Echtzeitschutz empfohlen wird. Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für Ihre Systemsicherheit. Die Bedrohung kann Ihr System nur dann beeinträchtigen, wenn die infizierten Datei aus einem Archiv extrahiert und ohne aktivierten Echtzeitschutz ausgeführt wird.

  Wenn Sie diese Option nutzen möchten, aktivieren Sie sie und schieben Sie den Regler bis zur maximal zulässigen Größe (in MB) der Archive, die bei Zugriff gescannt werden sollen.

- **E-Mails scannen.** Um zu verhindern, dass Bedrohungen auf Ihren Computer heruntergeladen werden, scannt Bitdefender automatisch eingehende und ausgehende E-Mails.

  Sie können zur Steigerung der Systemleistung die Bedrohungs-Scans für Ihre E-Mails deaktivieren, dies wird aber nicht empfohlen. Wenn Sie die entsprechenden Scan-Optionen deaktivieren, werden empfangene E-Mails und Dateien nicht gescannt. So kann es dazu kommen, dass infizierte Dateien auf Ihrem Computer gespeichert werden. Dies stellt keine größere Bedrohung dar, da der Echtzeitschutz die Bedrohung blockiert, wenn auf die infizierten Dateien zugegriffen wird (geöffnet, verschoben, kopiert oder ausgeführt).

- **Boot-Sektoren scannen.** Sie können Bitdefender einstellen, damit die Boot-Sektoren gescannt werden. Dieser Sektor der Festplatte beinhaltet den notwendigen Computercode um den Boot-Prozess zu starten. Wenn der Boot-Sektor durch eine Bedrohung infiziert wird, könnte das Laufwerk

unzugänglich werden und es könnte Ihnen nicht mehr möglich sein, Ihr System zu starten und auf Ihre Daten zuzugreifen.

- **Nur neue und geänderte Dateien.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.
- **Nach Keyloggern suchen.** Wählen Sie diese Option, um Ihr System auf Keylogger zu untersuchen. Keylogger zeichnen auf, was Sie auf Ihrer Tastatur tippen, und schicken dann via Internet Berichte an Hacker. Der Hacker kann über diese gestohlenen Daten sensible Informationen erfahren, so wie Kontonummern und Passwörter und kann Sie zu seinem eigenen Profit verwenden.
- **Bei Systemstart scannen.** Wählen Sie die Option **Früher Boot-Scan** aus, um Ihr System bei Systemstart sofort nach dem Laden aller wichtigen Dienste zu scannen. Diese Funktion sorgt für eine bessere Bedrohungserkennung beim Systemstart und beschleunigt diesen zugleich.

## Für gefundene Bedrohungen durchgeführte Aktionen

So können Sie einstellen, welche Aktionen der Echtzeitschutz durchführen soll:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **VIRENSCHUTZ**.
4. Klicken Sie im Fenster **SCHILD** auf das Akkordeonmenü **ERWEITERTE EINSTELLUNGEN ANZEIGEN**.

   Ein unterteiltes Fenster wird angezeigt.
5. Scrollen Sie im Fenster nach unten bis die Option **Aktionen nach Abschluss des Scans** erscheint.
6. Konfigurieren Sie die Scan-Einstellungen nach Ihren Wünschen.

Der Echtzeitschutz in Bitdefender kann die folgenden Aktionen durchführen:

**Aktionen ausführen**

Bitdefender wird je nach Art der infizierten Datei die empfohlenen Aktionen ausführen:

- **Infizierte Dateien.** Dateien, die als infiziert erkannt werden, stimmen mit einer in der Bitdefender-Datenbank gefunden Bedrohungsinformationen überein. Bitdefender wird automatisch versuchen, den Schad-Code aus der infizierten Datei zu entfernen und die Originaldatei zu rekonstruieren. Diese Operation bezeichnet man als Desinfektion.

  Dateien, die nicht desinfiziert werden können, werden in die Quarantäne verschoben, um so die Infizierung einzudämmen. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko. Weitere Informationen finden Sie unter *„Verwalten von Dateien in Quarantäne“* (S. 113).

  > **Wichtig**
  > Bestimmte Bedrohungsarten können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

- **Verdächtige Dateien.** Dateien werden von der heuristischen Analyse als verdächtig klassifiziert. Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist. Sie werden in Quarantäne verschoben, um eine mögliche Infektion zu verhindern.

  Dateien in Quarantäne werden standardmäßig an die Bitdefender-Labore geschickt, damit Sie dort von den Bitdefender-Bedrohungsforschern analysiert werden können. Wird das Vorhandensein einer Bedrohung bestätigt, werden die Bedrohungsinformationen per Update aktualisiert, damit die Bedrohung entfernt werden kann.

- **Archive mit infizierten Dateien.**
  - Archive, die nur infizierte Dateien enthalten, werden automatisch gelöscht.
  - Wenn ein Archiv sowohl infizierte als auch nicht infizierte Dateien enthält, wird Bitdefender versuchen, die infizierten Dateien zu löschen, vorausgesetzt, dass das Archiv mit den nicht infizierten Dateien wieder rekonstruiert werden kann. Wenn das Archiv nicht rekonstruiert werden kann, werden Sie benachrichtigt, dass keine Aktion durchgeführt werden kann, weil die Gefahr besteht, dass nicht infizierte Dateien verloren gehen.

**Dateien in Quarantäne verschieben**
Verschiebt die entdeckten Dateien in die Quarantäne. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko. Weitere Informationen finden Sie unter „*Verwalten von Dateien in Quarantäne*“ (S. 113).

**Zugriff verweigern**
Im Falle eines Virenfundes wird der Zugriff auf die Datei verhindert.

## Wiederherstellen der Standardeinstellungen

Die vorgegebenen Einstellungen zum Echtzeitschutz stellen einen guten Schutz gegen Bedrohungen bei nur minimaler Beeinträchtigung der Systemleistung sicher.

Um die vorgegebenen Echzeitschutz-Einstellungen wiederherzustellen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **VIRENSCHUTZ**.
4. Klicken Sie im Fenster **SCHILD** auf das Akkordeonmenü **ERWEITERTE EINSTELLUNGEN ANZEIGEN**.

   Ein unterteiltes Fenster wird angezeigt.
5. Scrollen Sie im Fenster nach unten bis die Option **Einstellungen zurücksetzen** erscheint. Wählen Sie diese Option aus, um die Virenschutzeinstellungen auf die Standardeinstellungen zurückzusetzen.

## 4.1.2. Bedarf-Scan

Die Aufgabe der Bitdefender-Software ist es sicherzustellen, dass es keine Bedrohungen in Ihrem System gibt. Dies wird erreicht, indem neue Bedrohungen ferngehalten und Ihre E-Mail-Nachrichten sowie alle heruntergeladenen oder auf Ihr System kopierten Dateien sorgfältig gescannt werden.

Es besteht aber die Gefahr, dass eine Bedrohung bereits in Ihrem System lauert, bevor Sie Bitdefender installieren. Deshalb sollten Sie Ihren Computer nach der Installation von Bitdefender auf bereits vorhandene Bedrohungen

prüfen. Übrigens sollten Sie Ihren Computer auch in Zukunft regelmäßig auf Bedrohungen prüfen.

Bedarf-Scans werden über Scan-Aufgaben ausgeführt. Die Scan-Aufgaben beinhalten die Scan-Optionen und die Objekte, die gescannt werden sollen. Sie können den Computer jederzeit scannen, indem Sie die Standard-Aufgaben oder Ihre eigenen Scan-Aufgaben (benutzerdefinierte Aufgaben) ausführen. Wenn Sie bestimmte Bereiche Ihres Computers scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierten Scan konfigurieren und ausführen.

## Eine Datei oder einen Ordner auf Bedrohungen prüfen

Wenn Sie den Verdacht hegen, dass Dateien und Verzeichnisse infiziert sein könnten, sollten Sie einen Scan durchführen. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner, die/den Sie scannen möchten, wählen Sie **Bitdefender** und dann **Mit Bitdefender scannen**. Der Viren-Scan-Assistent wird angezeigt. Er führt Sie durch den Scan-Vorgang. Wenn der Scan beendet wurde, werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.

## Durchführen von Quick Scans

Quick Scan setzt auf In-the-Cloud-Scans, um auf Ihrem System laufende Bedrohungen aufzuspüren. Die Ausführung eines Quick Scans dauert im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virenschutz-Scan in Anspruch nehmen würde.

So können Sie eine Quick Scan durchführen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Quick-Scan**.
4. Folgen Sie den Anweisungen des Viren-Scan-Assistenten, um den Scan abzuschließen. Bitdefender wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen. Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

Schneller noch geht es mit einem Klick auf das -Symbol im linken Seitenbereich der Bitdefender-Benutzeroberfläche, gefolgt von einem Klick auf die **Quick Scan**-Schaltfläche.

## Durchführen von System-Scans

Der System-Scan prüft den gesamten Computer auf alle Bedrohungsarten, die ein Sicherheitsrisiko darstellen, so zum Beispiel Malware, Spyware, Adware, Rootkits usw.

### Beachten Sie

Da ein **System-Scan** das gesamte System scannt, kann er eine Weile dauern. Es empfiehlt sich daher, diese Aufgabe durchzuführen, wenn Sie den Computer nicht benötigen.

Bevor Sie einen System-Scan ausführen, sollten Sie Folgendes beachten:

- Stellen Sie sicher, dass die Datenbank mit den Bedrohungsinformationen in Bitdefender jederzeit auf dem neuesten Stand ist. Wenn die Bedrohungsprüfung auf Grundlage einer Datenbank mit veralteten Bedrohungsinformationen erfolgt, kann dies verhindern, dass Bitdefender neue Bedrohungen erkennt, die seit dem letzten Update gefunden wurden. Weitere Informationen finden Sie unter *„Bitdefender auf dem neuesten Stand halten“ (S. 46)*.
- Schließen Sie alle geöffneten Programme.

Wenn Sie bestimmte Bereiche Ihres Computers scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierten Scan konfigurieren und ausführen. Weitere Informationen finden Sie unter *„Benutzerdefinierte Scans durchführen“ (S. 100)*.

So können Sie einen System-Scan durchführen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **VIRENSCHUTZ** auf **System-Scan**.
4. Bei der ersten Durchführung eines System-Scans werden Sie mit der Funktion vertraut gemacht. Klicken zum Fortfahren auf **OK, VERSTANDEN**.

5. Folgen Sie den Anweisungen des Viren-Scan-Assistenten, um den Scan abzuschließen. Bitdefender wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen. Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

## Benutzerdefinierte Scans durchführen

So können Sie einen benutzerdefinierten Scan im Detail konfigurieren und danach ausführen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Scans verwalten**.
4. Klicken Sie auf die Schaltfläche **Neue benutzerdefinierte Aufgabe**. Klicken Sie auf den Reiter **Basic**, um einen Namen für den Scan einzugeben und die Bereiche auszuwählen, die gescannt werden sollen.
5. Um die Scan-Optionen im Detail zu konfigurieren, wählen Sie den Reiter **Erweitert**. Ein neues Fenster wird angezeigt. Folgen Sie diesen Schritten:
   a. Sie können die Scan-Optionen einfach durch Einstellen der Scan-Tiefe festlegen. Schieben Sie den Regler dazu in die gewünschte Position. Die Beschreibung auf der rechten Seite der Skala helfen Ihnen, die Scan-Tiefe zu wählen, die für Ihre Bedürfnisse am besten geeignet ist.

      Erfahrene Benutzer können die Scan-Einstellungen von Bitdefender nutzen. Um die Scan-Optionen im Detail zu konfigurieren, klicken Sie auf **Benutzerdefiniert**. Weitere Informationen zu den Optionen finden Sie am Ende dieses Kapitels.

   b. Sie können auch folgende allgemeine Optionen konfigurieren:

      - **Aufgabe mit niedriger Priorität ausführen .** Verringert die Priorität des Scan-Vorgangs. Dadurch können andere Programme schneller laufen, der Scan dauert aber länger.
      - **Scan-Assistent in die Task-Leiste minimieren .** Minimiert das Scan-Fenster in die Task-Leiste Es kann durch einen Doppelklick auf das Bitdefender - Logo in der Symbolleiste wieder geöffnet werden.

- Wählen Sie die Aktion, die durchgeführt werden soll, wenn keine Bedrohungen gefunden wurden:

c. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

6. Klicken Sie im Fenster **Basic** auf den **Planen**-Schalter, um einen Zeitplan für Ihre Scan-Aufgabe festzulegen. Wählen Sie eine der entsprechenden Optionen, um einen Zeitplan festzulegen:
   - Start bei Systemneustart
   - Einmal
   - Periodisch
7. Klicken Sie auf **Scan starten** und folgen Sie den Anweisungen des Assistenten für den Viren-Scan, um den Scan abzuschließen. Abhängig von den Bereichen, die gescannt werden sollen, kann der Scan einige Zeit in Anspruch nehmen. Wenn der Scan beendet wurde, werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.
8. Bei Bedarf können Sie einen bereits durchgeführten benutzerdefinierten Scan einfach erneut ausführen, indem Sie auf den entsprechenden Eintrag in der Liste klicken.

## Informationen zu den Scan-Optionen

Diese Informationen sind vielleicht nützlich:

- Wenn Ihnen bestimmte Begriffe nicht geläufig sind, schlagen Sie diese im Glossar nach. Sie könne auch durch eine Suche im Internet hilfreiche Informationen finden.
- **Dateien prüfen.** Sie können Bitdefender so einstellen, dass alle Dateitypen oder nur Anwendungen (Programmdateien) gescannt werden. Das Scannen aller Dateien bietet den besten Schutz, während das Scannen nur von Anwendungen verwendet wird, um einen schnelleren Scan durchzuführen.

  Anwendungen (oder Programmdateien) sind weitaus anfälliger für Angriffe durch Bedrohungen als andere Dateitypen. Diese Kategorie beinhaltet die folgenden Dateierweiterungen: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek;

dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Scan-Optionen für Archive.** Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für Ihre Systemsicherheit. Die Bedrohung kann Ihr System nur dann beeinträchtigen, wenn die infizierten Datei aus einem Archiv extrahiert und ohne aktivierten Echtzeitschutz ausgeführt wird. Wir empfehlen jedoch, diese Option zu nutzen, um jegliche potentiellen Bedrohungen aufzuspüren und zu entfernen, auch wenn es sich nicht um unmittelbare Bedrohungen handelt.

  **Beachten Sie**
  Das Scannen archivierter Dateien erhöht die Gesamt-Scandauer und erfordert mehr Systemressourcen.

- **Boot-Sektoren scannen.** Sie können Bitdefender einstellen, damit die Boot-Sektoren gescannt werden. Dieser Sektor der Festplatte beinhaltet den notwendigen Computercode um den Boot-Prozess zu starten. Wenn der Boot-Sektor durch eine Bedrohung infiziert wird, könnte das Laufwerk unzugänglich werden und es könnte Ihnen nicht mehr möglich sein, Ihr System zu starten und auf Ihre Daten zuzugreifen.
- **Speicher scannen.** Wählen Sie diese Option, um Programme zu scannen, die im Speicher Ihres Systems laufen.
- **Registry scannen.** Wählen Sie diese Option, um die Registry-Schlüssel zu scannen. Die Windows-Registrierung ist eine Datenbank, in der Konfigurationseinstellungen und Optionen für die Windows-Betriebssystemkomponenten sowie für die installierten Anwendungen gespeichert sind.
- **Cookies scannen.** Wählen Sie diese Option, um die Cookies zu scannen, die von Ihrem Browser auf Ihrem Computer gespeichert werden.

- **Nur neue und geänderte Dateien.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.
- **Kommerzielle Keylogger ignorieren.** Wählen Sie diese Option, wenn Sie auf Ihrem Computer eine kommerzielle Keylogger-Software nutzen. Kommerzielle Keylogger sind seriöse Programme zur Überwachung des Computers, deren Hauptfunktion es ist, alle Tastatureingaben aufzuzeichnen.
- **Nach Rootkits suchen.** Wählen Sie diese Option, um nach Rootkits und Objekten zu suchen, die mit dieser Art von Software versteckt werden.

## Viren-Scan-Assistent

Wann immer Sie einen Bedarf-Scan starten (z. B. indem Sie mit der rechten Maustaste auf einen Ordner klicken, dann Bitdefender und anschließend **Mit Bitdefender scannen** wählen), wird der Bitdefender-Viren-Scan-Assistent eingeblendet. Folgen Sie den Anweisungen des Assistenten, um den Scan-Prozess abzuschließen.

### Beachten Sie

Falls der Scan-Assistent nicht erscheint, ist der Scan möglicherweise konfiguriert, im Hintergrund zu laufen. Sehen Sie nach dem Prüffortschritticon im Systemtray. Sie können dieses Objekt anklicken um das Scan-Fenster zu öffnen und so den Scan-Fortschritt zu sehen.

## Schritt 1 - Führen Sie den Scan durch

Bitdefender startet den Scan der aus gewählten Dateien und Verzeichnisse. Sie erhalten Echtzeitinformationen über den Scan-Status sowie Scan-Statistiken (einschließlich der bisherigen Laufzeit, einer Einschätzung der verbleibenden Laufzeit und der Anzahl der erkannten Bedrohungen).

Bitte warten Sie, bis Bitdefender den Scan beendet hat. Der Scan-Vorgang kann, abhängig von der Größe Ihrer Festplatte, eine Weile dauern.

**Einen Scan anhalten oder unterbrechen.** Sie können den Scan-Vorgang jederzeit durch einen Klick auf **STOPP** abbrechen. Sie gelangen dann direkt zum letzten Schritt des Assistenten. Um den Scan-Vorgang vorübergehend anzuhalten, klicken Sie einfach auf **PAUSE**. Um den Scan-Vorgang fortzusetzen klicken Sie auf **FORTSETZEN** .

**Passwortgeschützte Archive.** Wird ein passwortgeschütztes Archiv gefunden, werden Sie, abhängig von den Scan-Einstellungen, um die Eingabe des Passwortes gebeten. Mit Passwort geschützte Archive können nicht gescannt werden, außer wenn Sie das Passwort angeben. Die folgenden Optionen sind verfügbar:

- **Passwort.** Wenn Sie möchten, dass Bitdefender Archive scannt, wählen Sie diese Option aus und geben das Passwort an. Falls Sie das Passwort nicht kennen, wählen Sie eine der anderen Optionen.
- **Nicht nach Passwort fragen; das Objekt beim Scan überspringen.** Wählen Sie diese Option um das Scannen diesen Archivs zu überspringen.
- **Alle passwortgeschützte Dateien überspringen ohne diese zu scannen.** Wählen Sie diese Option, falls Sie nicht über passwortgeschützte Archive informiert werden möchten. Bitdefender kann diese Dateien und Objekte nicht scannen, erstellt aber einen Eintrag im Scan-Protokoll.

Wählen Sie die gewünschte Option aus und klicken Sie auf **OK**, um den Scan fortzusetzen.

## Schritt 2 - Wählen Sie entsprechende Aktionen aus

Wenn der Scan beendet wurde, werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.

### Beachten Sie

Wenn Sie einen Quick Scan oder einen System-Scan durchführen, wird Bitdefender während des Scans automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen. Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

Die infizierten Objekte werden nach Bedrohung sortiert in Gruppen angezeigt. Klicken Sie auf den Link, der der Bedrohung entspricht, um weitere Informationen über die infizierten Objekte zu erhalten.

Sie können eine umfassende Aktion für alle Probleme auswählen oder Sie können einzelne Aktionen für Problemgruppen auswählen. Eine oder mehrere der folgenden Optionen können im Menu erscheinen:

**Aktionen ausführen**

Bitdefender wird je nach Art der infizierten Datei die empfohlenen Aktionen ausführen:

- **Infizierte Dateien.** Dateien, die als infiziert erkannt werden, stimmen mit einer in der Bitdefender-Datenbank gefunden Bedrohungsinformationen überein. Bitdefender wird automatisch versuchen, den Schad-Code aus der infizierten Datei zu entfernen und die Originaldatei zu rekonstruieren. Diese Operation bezeichnet man als Desinfektion.

  Dateien, die nicht desinfiziert werden können, werden in die Quarantäne verschoben, um so die Infizierung einzudämmen. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko. Weitere Informationen finden Sie unter *„Verwalten von Dateien in Quarantäne“* (S. 113).

  **Wichtig**

  Bestimmte Bedrohungsarten können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

- **Verdächtige Dateien.** Dateien werden von der heuristischen Analyse als verdächtig klassifiziert. Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist. Sie werden in Quarantäne verschoben, um eine mögliche Infektion zu verhindern.

  Dateien in Quarantäne werden standardmäßig an die Bitdefender-Labore geschickt, damit Sie dort von den Bitdefender-Bedrohungsforschern analysiert werden können. Wird das Vorhandensein einer Bedrohung bestätigt, werden die Informationen per Update aktualisiert, damit die Bedrohung entfernt werden kann.

- **Archive mit infizierten Dateien.**
  - Archive, die nur infizierte Dateien enthalten, werden automatisch gelöscht.
  - Wenn ein Archiv sowohl infizierte als auch nicht infizierte Dateien enthält, wird Bitdefender versuchen, die infizierten Dateien zu löschen, vorausgesetzt, dass das Archiv mit den nicht infizierten Dateien wieder rekonstruiert werden kann. Wenn das Archiv nicht

rekonstruiert werden kann, werden Sie benachrichtigt, dass keine Aktion durchgeführt werden kann, weil die Gefahr besteht, dass nicht infizierte Dateien verloren gehen.

**Löschen**
Infizierte Dateien werden von der Festplatte entfernt.

Falls infizierte Dateien zusammen mit nicht infizierten Dateien in einem Archiv gespeichert sind, wird Bitdefender versuchen, die infizierten Dateien zu löschen und das Archiv mit den nicht infizierten Dateien zu rekonstruieren. Wenn das Archiv nicht rekonstruiert werden kann, werden Sie benachrichtigt, dass keine Aktion durchgeführt werden kann, weil die Gefahr besteht, dass nicht infizierte Dateien verloren gehen.

**Keine Aktion ausführen**
Es wird keine Aktion für die infizierte Dateien ausgeführt. Nachdem der Scan-Vorgang beendet wurde, können Sie das Scan-Protokoll öffnen um Informationen über diese Dateien anzuzeigen.

Klicken Sie auf **Fortfahren** um die festgelegten Aktionen anzuwenden.

### Schritt 3 - Zusammenfassung

Wenn Bitdefender die Probleme gelöst hat, wird eine Zusammenfassung der Scan-Ergebnisse in einem neuen Fenster angezeigt. Falls Sie umfangreichere Informationen zum Scan-Prozess möchten, klicken Sie auf **LOGDATEI ANZEIGEN**. Das Protokoll wird als .xml-Datei bereitgestellt und kann lokal gespeichert werden, indem Sie auf **Protokoll speichern** klicken und einen Speicherort auswählen.

#### Wichtig

In den meisten Fällen desinfiziert Bitdefender erfolgreich die aufgespürten infizierten Dateien oder er isoliert die Infektion. Dennoch gibt es Probleme, die nicht automatisch gelöst werden können. Bitte starten Sie Ihr System neu, wenn Sie dazu aufgefordert werden, damit der Bereinigungsprozess abgeschlossen werden kann. Weitere Informationen und eine Anleitung, wie Sie eine Bedrohung manuell entfernen können, finden Sie im Kapitel *„Entfernung von Bedrohungen“* (S. 223).

## Scan-Protokolle lesen

Bei jedem Scan wird ein Scan-Protokoll erstellt, und Bitdefender zeichnet die gefundenen Probleme im Fenster Virenschutz auf. Der Bericht enthält

detaillierte Informationen über den Scan-Vorgang, so wie Scan-Optionen, das Scan-Ziel, die gefundenen Bedrohungen und die Aktionen, die für diese Bedrohungen ausgeführt wurden.

Sobald der Scan beendet ist, können Sie das Scan-Protokoll direkt aus dem Scan-Assistenten heraus öffnen, indem Sie auf **PROTOKOLL ANZEIGEN** klicken.

So können Sie ein Scan-Protokoll oder gefundene Infektionen auch später anzeigen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wählen Sie unter dem Reiter **Alle** die Benachrichtigung bezüglich des neuesten Scans aus.

   Hier können Sie alle Ereignisse des Bedrohungs-Scans finden, einschließlich der Bedrohungen, die während Zugriff-Scans und vom Benutzer gestarteten Scans entdeckt wurden. Dazu kommen Statusänderungen für automatische Scans.
3. In der Benachrichtigungsliste können Sie überprüfen, welche Scans kürzlich durchgeführt wurden. Klicken Sie auf eine Benachrichtigung, um mehr darüber zu erfahren.
4. Um das Scan-Protokoll zu öffnen, klicken Sie auf **PROTOKOLL ANZEIGEN**.

### 4.1.3. Automatischer Scan von Wechselmedien

Bitdefender erkennt automatisch, wenn Sie Wechselmedien mit Ihrem Computer verbinden und scannt diese im Hintergrund, wenn die Auto-Scan-Option aktiviert wurde. Dies ist empfohlen, um die Infizierung Ihres Systems durch Bedrohungen zu verhindern.

Entdeckte Geräte fallen in eine dieser Kategorien:

- CDs/DVDs
- USB-Speichergeräte, sowie Flashstifte und externe Festplatten
- verbundene (entfernte) Netzlaufwerke

Sie können den automatischen Scan der Speichermedien eigens für jede Kategorie konfigurieren. Der automatische Scan der abgebildeten Netzlaufwerke ist standardmäßig deaktiviert.

## Wie funktioniert es?

Wenn ein Wechseldatenträger erkannt wird, beginnt Bitdefender diesen im Hintergrund auf Bedrohungen zu prüfen (vorausgesetzt, dass der automatische Scan für diesen Gerätetyp aktiviert ist). Das Bitdefender-Scan-Symbol erscheint in der Task-Leiste. Sie können dieses Objekt anklicken um das Scan-Fenster zu öffnen und so den Scan-Fortschritt zu sehen.

Wenn der Auto-Pilot aktiviert ist, läuft der Scan ohne Ihr Zutun. Der Scan wird lediglich protokolliert und Sie können die dazugehörigen Informationen im Fenster Benachrichtigungen abrufen.

Wenn der Autopilot deaktiviert ist:

1. Ein Pop-up-Fenster wird Sie darüber informieren, dass ein neues Gerät erkannt wurde und dass es derzeit gescannt wird.
2. In den meisten Fällen entfernt Bitdefender erkannte Bedrohungen automatisch oder isoliert infizierte Dateien in der Quarantäne. Sollte es nach dem Scan noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

   **Beachten Sie**
   Beachten Sie, dass keine Aktion gegen infizierte oder verdächtige Dateien auf CDs/DVDs vorgenommen werden kann. Ähnlich können keine Aktionen gegen infizierte oder verdächtige Dateien auf Netzlaufwerken vorgenommen werden, wenn Sie nicht die entsprechenden Freigaben haben.

3. Sobald der Scan abgeschlossen ist, wird das Fenster mit den Scan-Ergebnissen angezeigt, um Sie darüber zu informieren, ob Sie die Dateien auf dem Wechselmedium gefahrlos aufrufen können.

Diese Informationen könnten sich als hilfreich erweisen:

- Bitte gehen Sie vorsichtig vor, wenn Sie eine CD oder DVD nutzen, die mit Bedrohungen infiziert ist, da diese nicht von dem Datenträger entfernt werden kann (diese Medien sind schreibgeschützt). Stellen Sie sicher, dass der Echtzeitschutz aktiviert ist, um zu verhindern, dass Bedrohungen auf Ihr System gelangen. Es empfiehlt sich, wichtige Daten vom Datenträger auf Ihr System zu kopieren und den Datenträger dann zu entsorgen.
- Es kann vorkommen, dass Bitdefender nicht in der Lage ist, Bedrohungen aus juristischen oder technischen Gründen aus bestimmten Dateien zu

entfernen. Ein Beispiel hierfür sind Dateien, die mithilfe von proprietären Technologien archiviert wurden (der Grund dafür ist, dass das Archiv nicht korrekt wiederhergestellt werden kann).

Eine Anleitung zum Umgang mit Bedrohungen finden Sie im Kapitel *„Entfernung von Bedrohungen“ (S. 223)*.

### Verwalten des Scans für Wechselmedien

So können Sie Wechselmedien automatisch scannen:

Um den bestmöglichen Schutz zu garantieren, empfiehlt es sich, die **Auto-Scan-Option** für alle Arten von Wechselmedien zu aktivieren.

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **VIRENSCHUTZ**.
4. Wechseln Sie zum Reiter **LAUFWERKE UND GERÄTE**.

Die Prüfoptionen sind für bestmögliche Enteckungsraten vorkonfiguriert. Wenn infizierte Dateien erkannt werden, wird Bitdefender versuchen, diese zu desinfizieren (d. h. den Schad-Code zu entfernen) oder in die Quarantäne zu verschieben. Sollten beide Maßnahmen fehlschlagen, können Sie im Assistenten für den Virenschutz-Scan andere Aktionen für die infizierten Dateien festlegen. Die Prüfoptionen sind standartisiert, sie können daher nicht geändert werden.

## 4.1.4. Host-Datei scannen

Die Host-Datei ist standardmäßig Teil der Betriebssysteminstallation und dient der Zuordnung von Hostnamen zu IP-Adressen, wenn Sie neue Webseiten aufrufen oder Verbindungen mit FTP- und anderen Internet-Servern aufbauen. Dabei handelt es sich um eine reine Textdatei, die von Schadprogrammen verändert werden kann. Erfahrene Nutzer wissen, wie man damit lästige Werbeanzeigen, Banner, Cookies von Drittanbietern oder Datenjäger blockiert.

So können Sie die Option Host-Datei scannen konfigurieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.

2. Wechseln Sie zum Reiter **ERWEITERT**.
3. Klicken Sie auf die entsprechenden EIN/AUS-Schalter.

## 4.1.5. Konfiguration der Scan-Ausschlüsse

Mit Bitdefender können Sie bestimmte Dateien, Ordner oder Dateiendungen vom Scan ausschließen. Diese Funktion soll verhindern, dass Sie bei Ihrer Arbeit gestört werden und kann zudem dabei helfen, die Systemleistung zu verbessern. Ausschlüsse sollten nur von Benutzern eingesetzt werden, die erfahren im Umgang mit Computern sind oder wenn dies von einem Bitdefender-Mitarbeiter empfohlen wurde.

Sie können Ausschlüsse so konfigurieren, dass sie für Zugriff-Scans, Bedarf-Scans oder beide Arten von Scans gelten. Die ausgenommenen Objekte werden nicht geprüft, egal ob der Zugriff von Ihnen oder von einem Programm erfolgt.

### Beachten Sie

Ausschlüsse werden bei System- und Kontext-Scans NICHT berücksichtigt. Beim System-Scan handelt es sich um einen Bedarf-Scan, mit dem Sie das gesamte System nach Malware und Bedrohungen durchsuchen können, die die Sicherheit Ihrer Daten gefährden könnten. Kontextprüfung ist eine Art von On-Demand-Scan: Rechtsklicken Sie auf die zu scannende Datei oder das Verzeichnis und wählen Sie **Mit Bitdefender scannen**.

### Dateien und Ordner vom Scan ausschließen

So können Sie bestimmte Dateien und Ordner vom Scan ausschließen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **VIRENSCHUTZ**.
4. Wechseln Sie zum Reiter **AUSSCHLÜSSE**.
5. Klicken Sie auf das Akkordeonmenü **Vom Scan ausgeschlossene Dateien und Ordner**. Es erscheint ein Fenster. Hier können Sie die Dateien und Ordner verwalten, die vom Scan ausgeschlossen sind.
6. Fügen Sie Ausschlüsse hinzu, indem Sie die folgenden Schritte ausführen:

a. Klicken Sie auf die Schaltfläche **HINZUFÜGEN**.

b. Klicken Sie auf **Durchsuchen**, wählen Sie die Datei oder den Ordner, der vom Scan ausgeschlossen werden soll, und klicken Sie auf **OK**. Alternativ können Sie den Datei- oder Ordnerpfad auch manuell (oder per Kopieren und Einfügen) in das Bearbeitungsfeld eingeben.

c. Standardmäßig werden die ausgewählten Dateien oder Ordner sowohl vom Zugriff-Scan als auch vom Bedarf-Scan ausgeschlossen. Wählen Sie eine der anderen Optionen, um die Anwendung der Ausschlussregel anzupassen.

d. Klicken Sie auf **Hinzufügen**.

## Dateiendungen vom Scan ausschließen

Wenn Sie eine Dateiendung vom Scan ausschließen, wird Bitdefender Dateien mit dieser Endung unabhängig von ihrem Speicherort nicht mehr scannen. Der Ausschluss bezieht sich auch auf Dateien auf Wechselmedien, wie zum Beispiel CDs, DVDs, USB-Sticks oder Netzlaufwerke.

> **Wichtig**
> Lassen Sie Vorsichtig walten, wenn Sie Dateiendung vom Scan ausschließen, da solche Ausschlüsse Ihren Computer anfällig für Bedrohungen machen können.

Dateierweiterungen vom Scan ausschließen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **VIRENSCHUTZ**.
4. Wechseln Sie zum Reiter **AUSSCHLÜSSE**.
5. Klicken Sie auf das Akkordeonmenü **Vom Scan ausgeschlossene Dateiendungen**. In dem Fenster, das jetzt angezeigt wird, können Sie die Dateiendungen verwalten, die vom Scan ausgenommen sind.
6. Fügen Sie Ausschlüsse hinzu, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie auf die Schaltfläche **HINZUFÜGEN**.

b. Geben Sie die Dateiendungen ein, die vom Scan ausgeschlossen werden sollen. Trennen Sie einzelne Endungen mit einem Semikolon (;). Hier ein Beispiel:

   txt;avi;jpg

c. Standardmäßig werden alle Dateien mit den festgelegten Dateiendungen sowohl vom Zugriff-Scan als auch vom Bedarf-Scan ausgeschlossen. Wählen Sie eine der anderen Optionen, um die Anwendung der Ausschlussregel anzupassen.

d. Klicken Sie auf **Hinzufügen**.

## Verwalten von Scan-Ausschlüssen

Werden die konfigurierten Scan-Ausschlüsse nicht mehr benötigt, empfehlen wir, diese zu löschen oder die Scan-Ausschlüsse zu deaktivieren.

Verwaltung von Scan-Ausschlüssen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **VIRENSCHUTZ**.
4. Wechseln Sie zum Reiter **AUSSCHLÜSSE**.
5. Über die Optionen im Akkordeonmenü **Vom Scan ausgeschlossene Dateien und Ordner** können Sie die Scan-Ausschlüsse verwalten.
6. Um Scan-Ausschlüsse zu entfernen oder zu bearbeiten, klicken Sie auf einen der verfügbaren Links. Gehen Sie wie folgt vor:
   - Um einen Eintrag aus der Liste zu entfernen, markieren Sie ihn und klicken Sie danach auf **ENTFERNEN**.
   - Doppelklicken Sie auf einen Tabelleneintrag, um diesen zu bearbeiten (oder markieren Sie den Eintrag und klicken Sie dann auf **BEARBEITEN**). Ein neues Fenster wird angezeigt. Hier können Sie nach Bedarf festlegen, welche Dateiendungen oder -pfade bei welchem Scan-Typ ausgeschlossen werden sollen. Führen Sie die notwendigen Änderungen durch und klicken Sie dann auf **Ändern**.

## 4.1.6. Verwalten von Dateien in Quarantäne

Mit Bedrohungen infizierte Dateien, die nicht desinfiziert werden können, sowie verdächtige Dateien werden von Bitdefender in einem sicheren Bereich isoliert, der sogenannten Quarantäne. Bedrohungen in Quarantäne können keinen Schaden anrichten, da sie dort nicht geöffnet oder ausgeführt werden können.

Dateien in Quarantäne werden standardmäßig an die Bitdefender-Labore geschickt, damit Sie dort von den Bitdefender-Bedrohungsforschern analysiert werden können. Wird das Vorhandensein einer Bedrohung bestätigt, werden die Informationen per Update aktualisiert, damit die Bedrohung entfernt werden kann.

Zudem werden nach jedem Update der Datenbank mit den Bedrohungsinformationen die Dateien in der Quarantäne von Bitdefender gescannt. Gesäuberte Dateien werden automatisch an ihren Ursprungsort zurück gelegt.

So können Sie die Dateien in der Quarantäne einsehen und verwalten:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Quarantäne**.

   Hier finden Sie den Namen der Dateien in Quarantäne, ihren ursprünglichen Speicherort sowie den Namen der gefundenen Bedrohungen.
4. Dateien in Quarantäne werden von Bitdefender in Übereinstimmung mit den Standardeinstellungen für die Quarantäne automatisch verwaltet.

   Sie können die Quarantäneeinstellungen nach einem Klick auf **Einstellungen anzeigen** an Ihre Anforderungen anpassen, dies wird aber nicht empfohlen.

   Klicken Sie auf die Schalter, um das Folgende zu aktivieren oder deaktivieren:

   **Quarantäne nach Update der Malware-Signatur-Datenbank erneut scannen**
   Lassen Sie diese Option aktiviert, um Dateien in Quarantäne automatisch nach jedem Update der Bedrohungsinformationen zu scannen. Gesäuberte Dateien werden automatisch an ihren Ursprungsort zurück gelegt.

**Verdächtige Dateien in Quarantäne zur Analyse übermitteln**
Lassen Sie diese Option aktiviert, um Dateien in Quarantäne automatisch an das Bitdefender-Labor zu schicken. Die Beispieldateien werden dann von den Bitdefender-Bedrohungsforschern analysiert. Wird das Vorhandensein einer Bedrohung bestätigt, werden die Bedrohungsinformationen per Update aktualisiert, damit die Bedrohung entfernt werden kann.

**Inhalte löschen, die älter als 30 Tage sind**
Dateien in Quarantäne, die älter als 30 Tage sind, werden automatisch gelöscht.

**Ausschluss für wiederhergestellte Dateien erstellen**
Dateien, die Sie aus der Quarantäne wiederherstellen, werden ohne Reparatur an Ihren ursprünglichen Speicherort verschoben und bei zukünftigen Scans automatisch übersprungen.

5. Um eine Datei in Quarantäne zu löschen, markieren Sie diese und klicken dann auf **LÖSCHEN**. Wenn Sie eine Datei in Quarantäne am ursprünglichen Speicherort wiederherstellen möchten, klicken Sie zuerst auf die Datei und dann auf **WIEDERHERSTELLEN**.

## 4.2. Advanced Threat Defense

Die Bitdefender Erweiterte Gefahrenabwehr ist eine innovative und vorbeugende Erkennungstechnologie, die hoch entwickelte heuristische Methoden nutzt, um Ransomware und mögliche neue Bedrohungen in Echtzeit zu erkennen.

Die Erweiterte Gefahrenabwehr überwacht durchgehend alle auf Ihrem Computer laufenden Anwendungen auf Aktionen, die auf Bedrohungen hindeuten. Jede dieser Aktionen wird eingestuft, für jeden Prozess wird weiterhin eine Allgemeineinstufung erstellt.

Als zusätzliche Sicherheitsmaßnahme erhalten Sie eine Benachrichtigung über jeden erkannten und blockierten Ransomware-Angriff, auch dann, wenn der Autopilot aktiviert ist.

### Aktivieren oder Deaktivieren der Advanced Threat Defense

So aktivieren oder deaktivieren Sie die Advanced Threat Defense:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **ADVANCED THREAT DEFENSE** auf den EIN/AUS-Schalter.

**Beachten Sie**
Zum Schutz Ihrer Systeme vor Ransomware und anderen Bedrohungen empfehlen wir Ihnen, die Erweiterte Gefahrenabwehr nicht über einen längeren Zeitraum zu deaktivieren.

## Anzeigen von erkannten Ransomware-Angriffen

So können Sie die von der Erweiterten Gefahrenabwehr erkannten Ransomware-Angriffe einsehen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **ADVANCED THREAT DEFENSE** auf **Ransomware-Schutz**.
4. Bei der ersten Nutzung des Ransomware-Schutzes werden Sie mit der Funktion vertraut gemacht. Klicken zum Fortfahren auf **OK, VERSTANDEN**.

   Alle in den vergangenen 90 Tagen erkannten Angriffe werden angezeigt. Klicken Sie auf den entsprechenden Eintrag, um weitere Details zum erkannten Ransomware-Typ und den Dateipfad des schädlichen Prozesses anzuzeigen. Hier können Sie auch einsehen, ob die Desinfektion erfolgreich war.

## Erkannte verdächtige Apps anzeigen

So können Sie die von der Erweiterten Gefahrenabwehr erkannten verdächtigen Anwendungen einsehen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.

3. Klicken Sie im Bereich **ADVANCED THREAT DEFENSE** auf **Threat Defense**.
4. Beim ersten Aufrufen der Threat Defense werden Sie mit der Funktion vertraut gemacht. Klicken zum Fortfahren auf **OK, VERSTANDEN**.

   Alle in den vergangenen 90 Tagen als Bedrohung erkannten und blockierten Apps werden angezeigt. Klicken Sie auf den entsprechenden Eintrag, um weitere Details zu der App und den Dateipfad des schädlichen Prozesses anzuzeigen. Hier können Sie auch einsehen, ob die Desinfektion erfolgreich war.

## Hinzufügen von Prozessen zu den Ausschlüssen

Sie können Ausschlussregeln für vertrauenswürdige Anwendungen festlegen, damit die Erweiterte Gefahrenabwehr diese nicht blockiert, wenn ihr Verhalten auf eine Bedrohung hindeutet. Die Erweiterte Gefahrenabwehr wird ausgeschlossene Anwendungen auch weiterhin überwachen.

So fügen Sie Prozesse zur Ausschlussliste der Erweiterten Gefahrenabwehr hinzu:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **ADVANCED THREAT DEFENSE**.
4. Klicken Sie im Fenster **WHITELIST** auf **Anwendungen zur Whitelist hinzufügen**.
5. Suchen Sie die Anwendung, die ausgeschlossen werden soll, und klicken Sie auf **OK**.

   Entfernen Sie einen Eintrag aus der Liste, indem Sie auf die entsprechende **Entfernen**-Schaltfläche klicken.

# 4.3. Internet-Schutz

Der Bitdefender-Internet-Schutz lässt Sie sicher im Web surfen, indem er Sie vor potenziell schädlichen Seiten warnt.

Bitdefender bietet Echtzeit-Surf-Schutz für:

- Internet Explorer

- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari
- Bitdefender Safepay™
- Opera

So können Sie die Einstellungen für den Internet-Schutz konfigurieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **INTERNET-SCHUTZ**.

Klicken Sie auf die Schalter, um das Folgende zu aktivieren oder deaktivieren:

- HTTP-Datenverkehr scannen blockiert Bedrohungen aus dem Internet, so zum Beispiel auch Drive-by-Downloads.
- Suchberater, eine Komponente, die Ihre Suchmaschinentreffer und Links auf Seiten sozialer Netzwerke analysiert und bewertet. Die Bewertung wird durch ein Symbol neben dem Link oder Treffer angezeigt:

  Sie sollten diese Webseite nicht aufrufen.

  Diese Webseite könnte gefährliche Inhalte haben. Seien Sie vorsichtig, wenn Sie sie dennoch aufrufen möchten.

  Diese Seite ist sicher.

  Der Suchberater anaylsiert die Treffer der folgenden Internet-Suchmaschinen:
  - Google
  - Yahoo!
  - Bing
  - Baidu

  Der Suchberater bewertet Links, die auf den folgenden sozialen Netzwerken im Internet veröffentlicht werden:
  - Facebook
  - 109
- SSL scannen.

Gute durchdachte Angriffsversuche könnten den sicheren Datenverkehr für sich zu nutzen, um ihre Opfer zu täuschen. Darum empfiehlt es sich, den SSL-Scan zu aktivieren.

- Schutz vor Betrug.
- Schutz vor Phishing-Attacken.

Sie können eine Liste mit Websites anlegen, die von den Bitdefender-Engines für den Bedrohungs-, Phishing- und Betrugsschutz nicht gescannt werden sollen. Diese Liste sollte nur Websites enthalten, denen Sie uneingeschränkt vertrauen. Fügen Sie beispielsweise Websites hinzu, auf denen Sie häufig einkaufen.

So können Sie mit dem Internet-Schutz in Bitdefender Websites konfigurieren und verwalten:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **INTERNET-SCHUTZ** auf **Whitelist**.
4. Geben Sie den Namen der Website, die Sie der Whitelist hinzufügen möchten, in das **URL hinzufügen**-Textfeld ein und klicken Sie auf **Hinzufügen**.

   Um eine Website aus der Liste zu entfernen, wählen Sie sie aus der Liste aus und klicken Sie danach auf den entsprechenden **Entfernen**-Link.

   Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Fenster zu schließen.

## Bitdefender-Benachrichtigungen im Browser

Wenn Sie versuchen eine Website aufzurufen, die als unsicher eingestuft wurde, wird die entsprechende Website blockiert und eine Warnseite wird in Ihrem Browser angezeigt.

Die Seite enthält Informationen wie zum Beispiel die URL der Website und die erkannte Bedrohung.

Sie müssen entscheiden, wie Sie fortfahren möchten. Die folgenden Optionen sind verfügbar:

- Die Seite über einen Klick auf **Ich gehe lieber auf Nummer sicher** verlassen.

- Rufen Sie die Website trotz der Warnung auf, indem Sie auf **Ich bin mir der Risiken bewusst und möchte trotzdem fortfahren** klicken.

## 4.4. Spam-Schutz

Spam ist ein Begriff, den man für unaufgeforderte Emails verwendet. Spam ist ein wachsendes Problem für Heimanwender wie auch für Organisationen. Sie wollen wahrscheinlich nicht, dass Ihre Kinder die meisten dieser Spam-Mails mit häufig pornographischem Inhalt lesen oder dass Sie deswegen sogar in Unannehmlichkeiten geraten. Spam wird immer mehr zum Ärgernis. Daher ist es das Beste, diese Mails gar nicht mehr zu erhalten.

Bitdefender Antispam greift auf außergewöhnliche technologische Innovationen und Standard-Antispam-Filter zurück, um Spams auszusortieren, bevor dieser im Posteingang landen. Weitere Informationen finden Sie unter *„Wie funktioniert der Spam-Schutz?“* (S. 120).

Der Bitdefender Antispam-Schutz ist nur für Email Clients verfügbar, die Emails über das POP3-Protokoll zu empfangen. POP3 ist eines der am meisten benutzten Protokolle für das Downloaden der E-Mail-Nachrichten vom Mail-Server.

### Beachten Sie

Bitdefender bietet keinen Antispam-Schutz für Email-Konten, auf die Sie über einen web-basierten Email-Service zugreifen.

Von Bitdefender aufgespürte Spams werden in der Betreffzeile mit dem [spam]-Marker gekennzeichnet. Bitdefender legt Spam-Nachrichten automatisch in einem festgelegten Verzeichnis ab, wie folgt:

- In Microsoft Outlook werden Spams in den **Spam** Ordner verschoben. Dieser ist unter **gelöschte Objekte** zu finden. Der **Spam**-Ordner wird erstellt, wenn eine E-Mail als Spam markiert wurde.
- Im Mozilla Thunderbird, werden Spams in den **Spam** Ordner verschoben, der unter **Trash** Ordner zu finden ist. Der **Spam**-Ordner wird erstellt, wenn eine E-Mail als Spam markiert wurde.

Falls Sie andere E-Mail-Clients verwenden, müssen Sie eine Regel erstellen, um Nachrichten, die von Bitdefender als [spam] markiert wurden, in einen eigens erstellten Quarantäne-Ordner zu verschieben. Wenn die Ordner „Gelöschte Objekte“ oder „Papierkorb“ gelöscht werden, wird auch der Spam-Ordner gelöscht. Es wird jedoch ein neuer Spam-Ordner erstellen, wenn wieder eine E-Mail als Spam markiert wird.

## 4.4.1. Wie funktioniert der Spam-Schutz?

### AntiSpam Filter

Die Bitdefender-Spamschutz-Engine nutzt Cloud-Schutz und eine Reihe verschiedener Filter, um Ihren Posteingang frei von SPAM zu halten, so zum Beispiel die Freundesliste, Spammer-Liste und Zeichensatz-Filter..

### Freundesliste/ Spammer-Liste

Viele Menschen kommunizieren normalerweise mit einer bestimmten Gruppe von Menschen oder aber erhalten Nachrichten von Firmen oder Organisationen mit derselben Domain. Wird eine **Freunde-/Spammerliste** geführt, so können Sie festlegen, welche Emails Sie erhalten wollen (die von Freunden) und welche Sie nicht erhalten möchten (die von Spammern).

#### Beachten Sie

Wir empfehlen, dass Sie die Namen Ihrer Freunde und deren Email-Adressen der **Freundesliste** hinzufügen, damit sichergestellt wird, dass nur solche Emails an Sie weitergeleitet werden. Bitdefenderblockiert keine Nachrichten dieser Absender. Somit stellt die Liste der Freunde sicher, dass alle legitimen Nachrichten auch ankommen.

### Zeichensatz-Filter

Viele der Spam-Mails sind in Kyrillisch und/oder Asiatisch geschrieben. Der Zeichensatz-Filter erkennt diese Art von Nachrichten und markiert sie als SPAM.

### Spam-Schutz

Die Bitdefender Antispam Engine kombiniert alle Antispam-Filter um festzustellen, ob eine bestimmte Email in den **Posteingang** gelangen sollte, oder nicht.

Jede E-Mail, die aus dem Internet kommt, wird zuerst mit den Filtern Freundesliste/Spammerliste überprüft. Falls die Adresse des Absenders in der Freundesliste gefunden wird, wird diese E-Mail direkt in Ihren **Posteingang** verschoben.

Wenn nicht, überprüft der Filter Spammerliste, ob der Absender der E-Mail auf der Liste der Spammer steht. Falls dem so ist, wird die E-Mail als Spam markiert und in den **Spam**-Ordner verschoben.

Der Zeichensatz-Filter überprüft, ob die E-Mail in kyrillischen oder asiatischen Zeichen geschrieben wurde. Falls dem so ist, wird die E-Mail als Spam markiert und in den **Spam**-Ordner verschoben.

**Beachten Sie**
Wenn die Email in der Betreffzeile als „ausdrücklich sexuell" gekennzeichnet wurde, stuft Bitdefender die Email als Spam ein.

### Unterstützte E-Mail-Clients und Protokolle

Der Antispam-Schutz steht für alle POP3/SMTP E-Mail-Clients zur Verfügung. Die Bitdefender Antispam-Toolbar wird integriert in:

- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Ab Mozilla Thunderbird 14

## 4.4.2. Aktivieren / Deaktivieren des Spam-Schutzes

Der Spam-Schutz ist standardmäßig aktiviert.

So können Sie die Spam-Schutz-Funktion deaktivieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **SPAM-SCHUTZ** auf den AN/AUS-Schalter.

## 4.4.3. Verwenden der Spam-Schutz-Symbolleiste in Ihrem Mail-Client-Fenster

Im oberen Teil Ihres Mail Client Fensters können Sie die Antispamleiste sehen. Diese hilft Ihnen beim Verwalten des Antispamschutzes direkt vom E-Mail Client aus. Sie können Bitdefender ganz einfach korrigieren, falls eine reguläre Mail als Spam markiert wurde.

**Wichtig**
Bitdefender integriert sich in die gebräuchlichsten Mail Clients durch eine einfach zu verwendende Antispam-Symbolleiste. Um die komplette Liste der unterstützen E-Mail Clients zu erhalten, lesen Sie bitte: *„Unterstützte E-Mail-Clients und Protokolle"* (S. 121).

Unten stehend finden Sie eine Beschreibung aller Buttons der Bitdefender-Symbolleiste:

**Einstellungen** - Öffnet eine Fenster, in dem Sie die Spam-Filter und die Einstellungen für die Symbolleiste konfigurieren können.
**Ist Spam** - Gibt an, dass es sich bei der ausgewählten E-Mail um Spam handelt. Die E-Mail wird sofort in den **Spam**-Ordner verschoben. Wenn die Cloud-Dienste für den Spam-Schutz aktiviert sind, wird die Nachricht zur weiteren Analyse in die Bitdefender-Cloud geschickt.
**Kein Spam** - Zeigt an, dass es sich bei der angezeigten E-Mail nicht um Spam handelt und dass Bitdefender sie nicht als solche hätte kennzeichnen sollen. Die E-Mail wird aus dem **Spam** Ordner ins **Inbox** Ordner verschoben. Wenn die Cloud-Dienste für den Spam-Schutz aktiviert sind, wird die Nachricht zur weiteren Analyse in die Bitdefender-Cloud geschickt.

**Wichtig**
Der Button **Kein Spam** wird aktiv, wenn Sie eine Nachricht als Spam markiert haben von Bitdefender (normalerweise werden diese Nachrichten in den **Spam**-Verzeichnis verschoben).

**Neuer Spammer** - fügt den Absender der ausgewählten E-Mail zur Liste der Spammer hinzu. Klicken Sie zur Bestätigung **OK**. Die E-Mail-Nachrichten, empfangen von den Adressen aus der Spammerliste, werden automatisch als [spam] markiert.
**Neuer Freund** - fügt den Sender der ausgewählten E-Mail der Liste der Freunde hinzu. Klicken Sie zur Bestätigung **OK**. Sie werden jetzt immer E-Mails von diesem Absender erhalten, egal welchen Inhalts.
**Spammer** - Öffnen Sie **Spammerliste**. Sie enthält alle E-Mail-Adressen, von denen Sie keine Nachricht erhalten wollen, gleichwelchen Inhalts. Weitere Informationen finden Sie unter *„Konfigurieren der Spammerliste“* (S. 125).
**Freunde** - Öffnen Sie die **Freundesliste**. Sie enthält alle E-Mail-Adressen, von denen Sie immer Nachrichten erhalten wollen, gleichwelchen Inhalts. Weitere Informationen finden Sie unter *„Konfigurieren der Freundesliste“* (S. 124).

## Anzeigen von Erkennungsfehlern

Wenn Sie einen unterstützten E-Mail-Client verwenden, können Sie den Spam-Filter einfach korrigieren (indem Sie angeben, welche E-Mails nicht als [spam] hätten markiert werden sollen). Dadurch wird die Effizienz des Spam-Filters verbessert. Folgen Sie diesen Schritten:

1. Öffnen Sie den Mail Client.
2. Gehen Sie zu dem Junk Mail Ordner, wo die Spam Nachrichten hin verschoben werden.
3. Wählen Sie die Nachricht, die von Bitdefender fälschlicherweise als [spam] markiert wurde, aus.
4. Klicken Sie auf **Neuer Freund** in der Bitdefender-Spam-Schutz-Symbolleiste. Klicken Sie zur Bestätigung **OK**. Sie werden jetzt immer E-Mails von diesem Absender erhalten, egal welchen Inhalts.
5. Klicken Sie in der Bitdefender-Spam-Schutz-Symbolleiste (die sich üblicherweise im oberen Teil des Mail-Client-Fensters befindet) auf die Schaltfläche **Kein Spam**. Die E-Mail wird in den Posteingangsordner verschoben.

## Hinweisen auf unerkannte Spam-Nachrichten

Wenn Sie einen unterstützten E-Mail-Client verwenden, können Sie einfach angeben, welche E-Mails als Spam hätten markiert werden sollen. Dadurch wird die Effizienz des Spam-Filters verbessert. Folgen Sie diesen Schritten:

1. Öffnen Sie den Mail Client.
2. Begeben Sie sich zum Inbox Ordner.
3. Wählen Sie die unentdeckte Spam-Nachricht.
4. Klicken Sie in der Bitdefender-Spam-Schutz-Symbolleiste (die sich üblicherweise im oberen Teil des Mail-Client-Fensters befindet) auf die Schaltfläche **Ist Spam**. Sie werden dann sofort als [spam] markiert und in den Junk-Ordner verschoben.

## Konfigurieren der Symbolleisteneinstellungen

Um die Einstellungen für die Spam-Schutz-Symbolleiste in Ihrem E-Mail-Client zu konfigurieren, klicken Sie in der Symbolleiste auf die Schaltfläche **Einstellungen** und danach auf den Reiter **Symbolleisteneinstellungen**.

Dabei haben Sie die folgenden Möglichkeiten:

- **Markieren Sie Spam-E-Mail Nachrichten als 'gelesen'** - Markiert die Spam-Nachrichten automatisch als gelesen, so dass sie Sie nicht stören, wenn diese ankommen.

- Sie können festlegen, ob Bestätigungsfenster angezeigt werden sollen, wenn Sie in der Spam-Schutz-Symbolleiste die Schaltflächen **Neuer Spammer** und **Neuer Freund** anklicken.

  Bestätigungsfenster verhindern, dass Sie die Absender von E-Mail-Nachrichten versehentlich zu Ihrer Freundes- bzw. Spam-Liste hinzufügen.

## 4.4.4. Konfigurieren der Freundesliste

Die **Liste der Freunde** ist eine Liste, die alle E-Mail-Adressen enthält, von denen Sie immer Nachrichten erhalten möchten, egal, welchen Inhalt sie haben. Nachrichten Ihrer Freunde werden nicht als Spam markiert, auch wenn der Inhalt dem von Spam ähnlich sein sollte.

### Beachten Sie

Jede Mail von einer Adresse Ihrer **Freundesliste** wird automatisch in Ihren Posteingang verschoben.

Konfigurierung und Verwaltung der Freundesliste:

- Wenn Sie Microsoft Outlook oder Thunderbird nutzen, klicken Sie in der Bitdefender-Spam-Schutz-Symbolleiste auf die Schaltfläche **Freunde**.
- Alternativ:
  1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
  2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
  3. Klicken Sie im Bereich **SPAM-SCHUTZ** auf **Freunde verwalten**.

Um eine E-Mail-Adresse hinzuzufügen, wählen Sie die Option **E-Mail-Adresse** und klicken Sie dann auf **Hinzufügen**. Syntax: name@domain.com.

Um alle E-Mail-Adressen einer bestimmten Domain hinzuzufügen, wählen Sie die Option **Domain-Name**, geben Sie den Domain-Namen ein und klicken Sie auf **Hinzufügen**. Syntax:

- @domain.com und domain.com - alle eingehenden Mails von domain.com werden in Ihren **Posteingang** verschoben, gleich welchen Inhalts;
- domain - alle eingehenden Mails von domain (egal welcher Endung) werden als Spam markiert;
- com - alle Mails mit dieser Endung com werden als Spam markiert;

Wir empfehlen, keine kompletten Domains hinzuzufügen, in einigen Situationen kann dies jedoch sinnvoll sein. Sie können beispielsweise die Email-Domain der Firma, für die Sie arbeiten, oder die von vertrauenswürdigen Partnern hinzufügen.

Um ein Objekt aus der Liste zu löschen, klicken Sie auf den entsprechenden **Entfernen**-Link. Klicken Sie auf **Liste leeren**, um alle Einträge aus der Liste zu löschen.

Sie können die Liste der Freunde speichern, so das diese auf einem anderen Rechner oder nach einer Neuinstallation benutzt werden kann. Um die Freundesliste aufzunehmen, klicken Sie auf **Speichern** und wählen Sie den gewünschten Ort. Die Datei wird .bwl als Erweiterung haben.

Um eine zuvor gespeicherte Freundesliste zu laden, klicken Sie **Laden** und öffnen die entsprechende .bwl Datei. Um den Inhalt einer aktuellen Liste zurückzusetzen während der Inhalt einer zuvor gespeicherten Liste geladen wird, wählen Sie **Liste überschreiben**.

Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

## 4.4.5. Konfigurieren der Spammerliste

**Liste der Spammer** - Liste die alle E-Mail-Adressen enthält, von denen Sie keine Nachrichten erhalten wollen, gleich welchen Inhalts. Jede Mail von einer Adresse Ihrer **Spammerliste** wird automatisch als Spam markiert.

Konfigurierung und Verwaltung der Spammer-Liste:

- Wenn Sie Microsoft Outlook oder Thunderbird nutzen, klicken Sie in der in den Mail-Client integrierten Bitdefender-Spam-Schutz-Symbolleiste auf die Schaltfläche **Spammer**.
- Alternativ:
  1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
  2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
  3. Klicken Sie im Bereich **SPAM-SCHUTZ** auf **Spammer verwalten**.

Um eine E-Mail-Adresse hinzuzufügen, wählen Sie die Option **E-Mail-Adresse** und klicken Sie dann auf **Hinzufügen**. Syntax: name@domain.com.

Um alle E-Mail-Adressen einer bestimmten Domain hinzuzufügen, wählen Sie die Option **Domain-Name**, geben Sie den Domain-Namen ein und klicken Sie auf **Hinzufügen**. Syntax:

- @domain.com und domain.com - alle eingehenden Mails von domain.com werden in Ihren **Posteingang** verschoben, gleich welchen Inhalts;
- domain - alle eingehenden Mails von domain (egal welcher Endung) werden als Spam markiert;
- com - alle Mails mit dieser Endung com werden als Spam markiert.

Wir empfehlen, keine kompletten Domains hinzuzufügen, in einigen Situationen kann dies jedoch sinnvoll sein.

**Warnung**

Fügen Sie keine legitimen Web-Mail-Anbieter (wie z. B. Gmail, GMX oder Web.de) zur Spammer-Liste hinzu. Sonst werden sämtliche E-Mails aller Benutzer solcher Anbieter als Spam eingestuft. z.B: wenn Sie yahoo.com zu Spammerliste hinzufügen, werden alle E-Mails die von yahoo.com Adressen kommen, als [spam] markiert.

Um ein Objekt aus der Liste zu löschen, klicken Sie auf den entsprechenden **Entfernen**-Link. Klicken Sie auf **Liste leeren**, um alle Einträge aus der Liste zu löschen.

Sie können die Spammer Liste in eine Datei sichern, damit Sie sie nach einer Neuinstallation oder auf einem anderen Computer nutzen können. Um die Spammerliste aufzunehmen, klicken Sie auf **Speichern** und wählen Sie den gewünschten Ort. Die Datei wird .bwl als Erweiterung haben.

Um eine zuvor gespeicherte Spammerliste zu laden, klicken Sie **Laden** und öffnen die entsprechende .bwl Datei. Um den Inhalt einer aktuellen Liste zurückzusetzen während der Inhalt einer zuvor gespeicherten Liste geladen wird, wählen Sie **Liste überschreiben**.

Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

## 4.4.6. Konfigurieren der lokalen Spam-Schutz-Filter

Wie in *„Wie funktioniert der Spam-Schutz?“ (S. 120)* beschrieben, nutzt Bitdefender eine Kombination aus unterschiedlichen Spam-Filtern, um Spam zu identifizieren. Die Spam-Filter sind für den effizienten Schutz vorkonfiguriert.

### Wichtig

Abhängig davon, ob Sie legitime Emails mit asiatischen oder kyrillischen Zeichen erhalten, aktivieren oder deaktivieren Sie die Einstellung, die solche Emails automatisch abblockt. Die entsprechende Einstellung ist in den lokalisierten Programmversion deaktiviert, die solche Zeichensätze verwendet (wie z. B. in der russischen oder chinesischen Programmversion).

So können Sie die lokalen Spam-Schutz-Filter konfigurieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **SPAM-SCHUTZ**.
4. Klicken Sie auf die entsprechenden AN/AUS-Schalter.

Wenn Sie Microsoft Outlook oder Thunderbird nutzen, können Sie die lokalen Spam-Filter direkt aus Ihrem Mail-Client heraus konfigurieren. Klicken Sie in der Bitdefender-Spam-Schutz-Symbolleiste (die sich üblicherweise im oberen Teil des Mail-Client-Fensters befindet) auf die Schaltfläche **Einstellungen** und wählen Sie dann den Reiter **Spam-Filter** aus.

## 4.4.7. Konfigurieren der Cloud-Einstellungen

Die Cloud-Erkennung nutzt die Bitdefender-Cloud-Dienste, um Ihnen effizienten und stets aktuellen Spam-Schutz bieten zu können.

Der Cloud-Schutz funktioniert, solange der Bitdefender-Spam-Schutz aktiviert ist.

Beispiele legitimer E-Mails und Spam-Nachrichten können an die Bitdefender-Cloud geschickt werden, wenn Sie auf Erkennungsfehler oder unerkannte Spam-Nachrichten hinweisen. Dies trägt dazu bei, die Bitdefender-Spam-Erkennung zu verbessern.

Konfigurieren Sie die Übermittlung der E-Mail-Beispiele an die Bitdefender-Cloud, indem Sie die gewünschten Optionen wie folgt auswählen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.

3. Klicken Sie auf das ⚙-Symbol unten rechts im Bereich **SPAM-SCHUTZ**.
4. Wählen Sie im Fenster **EINSTELLUNGEN** die gewünschten Optionen aus.

Wenn Sie Microsoft Outlook oder Thunderbird nutzen, können Sie die Cloud-Erkennung direkt aus Ihrem Mail-Client heraus konfigurieren. Klicken Sie in der Bitdefender-Spam-Schutz-Symbolleiste (die sich üblicherweise im oberen Teil des Mail-Client-Fensters befindet) auf die Schaltfläche ⚙ **Einstellungen** und wählen Sie dann den Reiter **Cloud-Einstellungen** aus.

## 4.5. Firewall

Die Firewall schützt Ihren Computer vor unerwünschten Verbindungen von innen und außen sowohl im lokalen Netzwerk als auch im Internet. Sie funktioniert im Prinzip wie ein Wächter an Ihrem Tor - sie überwacht alle Verbindungsversuche und entscheidet, welche Verbindungen zugelassen und welche blockiert werden.

Die Bitdefender-Firewall nutzt eine Regelwerk, um den eingehenden und ausgehenden Datenverkehr auf Ihrem System zu filtern.

Unter normalen Umständen legt Bitdefender automatisch eine Regel an, sobald eine Anwendung versucht, auf das Internet zuzugreifen. Sie können Anwendungsregeln zudem manuell hinzufügen oder bearbeiten.

Als zusätzliche Sicherheitsmaßnahme erhalten Sie eine Benachrichtigung über jeden Versuch einer schädlichen Anwendung, auf das Internet zuzugreifen, auch dann, wenn der Autopilot aktiviert ist.

Bitdefender ordnet automatisch jeder erkannten Netzwerkverbindung den entsprechenden Netzwerktyp zu. Je nach Netzwerktyp wird der Firewall-Schutz für jede Verbindung auf die angemessene Stufe eingestellt.

Um mehr über die Firewall-Einstellungen für jeden Netzwerktyp und die Bearbeitung der Netzwerkeinstellungen zu erfahren, lesen Sie bitte das Kapitel *„Verbindungseinstellungen verwalten“ (S. 132)*.

### Aktivieren / Deaktivieren des Firewall-Schutzes

So können Sie den Firewall-Schutz aktivieren oder deaktivieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das Ⓑ-Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.

3. Klicken Sie im Bereich **FIREWALL** auf den EIN/AUS-Schalter.

**Warnung**

Die Deaktivierung der Firewall sollte immer nur von kurzer Dauer sein, da Ihr Computer so der Gefahr durch nicht autorisierte Verbindungen ausgesetzt wird. Aktivieren Sie die Firewall so schnell wie möglich wieder.

### 4.5.1. Verwalten von App-Regeln

So können Sie die Firewall-Regeln anzeigen und verwalten, die den Zugang von Anwendungen zu Netzwerkressourcen und dem Internet steuern:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **FIREWALL** auf **Anwendungszugriff**.
4. Beim ersten Aufrufen der Firewall werden Sie mit der Funktion vertraut gemacht. Klicken zum Fortfahren auf **OK, VERSTANDEN**.

Sie können eine Übersicht der letzten 15 Programme (Prozesse) einsehen, die die Bitdefender-Firewall und das Internet-Netzwerk, mit dem Sie verbunden sind, durchlaufen haben. Um die Regeln einzusehen, die für eine bestimmte Anwendung erstellt wurden, klicken Sie auf den entsprechenden Eintrag und danach auf den Link **Anwendungsregeln anzeigen**. Das Fenster **REGELN** wird angezeigt.

Für jede Regel werden die folgenden Informationen angezeigt:

- **NETZWERK** - Der Prozess und die Netzwerkadaptertypen (Heim / Büro, Öffentlich oder Alle), auf die die Regel angewendet wird. Regeln werden automatisch erstellt um den Netzwerk- oder Internetzugriff jedes Adapters zu filtern. Die Regeln werden standardmäßig auf jedes Netzwerk angewendet. Sie können manuell Regeln erstellen oder bestehende Regeln bearbeiten um den Zugriff einer Anwendung auf das Netzwerk/Internet über einen speziellen Adapter zu filtern (zum Beispiel ein drahtloser Netzwerkadapter).
- **PROTOKOLL** - Das IP-Protokoll, auf das die Regel angewendet wird. Die Regeln werden standardmäßig auf jedes Protokoll angewendet.
- **DATENVERKEHR** - Die Regel wird in beide Richtungen angewendet, eingehend und ausgehend.

- **PORTS** - Das PORT-Protokoll, auf das die Regel angewendet wird. Die Regeln werden standardmäßig auf alle Ports angewendet.
- **PORTS** - Das Internet-Protokoll (IP), auf das die Regel angewendet wird. Die Regeln werden standardmäßig auf alle IP-Adressen angewendet.
- **ZUGRIFF** - Gibt an, ob der Zugriff der Anwendung auf das Netzwerk oder das Internet unter den festgelegten Umständen zugelassen oder verweigert wird.

Klicken Sie auf das ··· -Symbol, um die Regeln für die ausgewählte App zu bearbeiten oder zu löschen.

- **Regel bearbeiten** - Öffnet ein Fenster, in dem die aktuelle Regel bearbeitet werden kann.
- **Regel löschen** - Hiermit können Sie den vorhandenen Regeln für die ausgewählte App löschen.

## Hinzufügen von App-Regeln

Gehen Sie zum Hinzufügen einer App-Regel folgendermaßen vor:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **FIREWALL**.
4. Klicken Sie oben im Fenster **REGELN** auf **Regel hinzufügen**.

Im Fenster **EINSTELLUNGEN** können Sie die folgenden Änderungen vornehmen:

- **Diese Regel auf alle Anwendungen anwenden.** Aktivieren Sie diese Option, um die Regel auf alle Anwendungen anzuwenden.
- **Programmpfad.** Klicken Sie auf **Durchsuchen** und wählen Sie das Programm für das die Regel angewendet wird.
- **Berechtigung.** Wählen Sie eine der verfügbaren Berechtigungs-Optionen:

| Berechtigung | Beschreibung |
|---|---|
| **Zulassen** | Der eingestellten Anwendung wird die Verbindung unter den angegebenen Umständen erlaubt. |

| Berechtigung | Beschreibung |
|---|---|
| **Verweigern** | Der eingestellten Anwendung wird die Verbindung unter den angegebenen Umständen verweigert. |

- **Netzwerktyp.** Wählen Sie den Netzwerktyp aus, auf den die Regel angewendet werden soll. Sie können den Netzwerktyp ändern, indem Sie das Dropdown-Menü unter **Netzwerktyp** öffnen und einen der verfügbaren Netzwerktypen aus der Liste auswählen.

| Netzwerktyp | Beschreibung |
|---|---|
| **Alle Netzwerke** | Unabhängig vom Netzwerktyp sämtlichen Datenverkehr zwischen Ihrem Computer und anderen Computern zulassen. |
| **Heim/Büro** | Erlaubt den Datenverkehr zwischen Ihrem Computer und den Computern im lokalen Netzwerk. |
| **Öffentlich** | Sämtlicher Datenverkehr wird gefiltert. |

- **Protokoll.** Wählen Sie aus dem Menu das IP-Protokoll für das die Regel angewendet wird.
  - Wenn Sie möchten, dass die Regel für alle Protokolle angewendet wird, wählen Sie **Alle**.
  - Wenn Sie möchten, dass die Regel für TCP-Protokolle angewendet wird, wählen Sie **TCP**.
  - Wenn Sie möchten, dass die Regel für UDP-Protokolle angewendet wird, wählen Sie **UDP**.
  - Wenn Sie möchten, dass die Regel für ICMP angewendet wird, wählen Sie **ICMP** aus.
  - Wenn Sie möchten, dass die Regel für IGMP angewendet wird, wählen Sie **IGMP** aus.
  - Wenn Sie möchten, dass die Regel auf ein bestimmtes Protokoll angewendet wird, geben Sie die Nummer des Protokolls, das Sie filtern möchten, in das leere Feld ein.

> **Beachten Sie**
>
> Die Nummern von IP-Protokollen werden von der Internet Assigned Numbers Authority (IANA) zugewiesen. Die komplette Liste zugewiesener Nummern von IP-Protokollen finden Sie unter http://www.iana.org/assignments/protocol-numbers.

- **Richtung.** Wählen Sie aus dem Menu die Richtung des Datenverkehrs, für den die Regel angewendet wird.

| Richtung | Beschreibung |
|---|---|
| **Ausgehend** | Die Regel bezieht sich nur auf den ausgehenden Datenverkehr. |
| **Eingehend** | Die Regel bezieht sich nur auf den eingehenden Datenverkehr. |
| **Beides** | Die Regel findet in beiden Richtungen Anwendung. |

Im Fenster **ERWEITERT** können Sie die folgenden individuellen Einstellungen vornehmen:

- **Benutzerdefinierte lokale Adresse.** Geben Sie die lokale IP-Adresse und den Port an, auf den die Regel angewendet werden soll.
- **Benutzerdefinierte Remoteadresse.** Geben Sie die Remote-IP-Adresse und den Port an, auf den die Regel angewendet werden soll.

Um die vorhandenen Regeln zu entfernen und die Standardregeln wiederherzustellen, klicken Sie oben im Fenster **REGELN** auf den Link **Regeln zurücksetzen**.

## 4.5.2. Verbindungseinstellungen verwalten

Je nachdem, ob Sie Ihre Internetverbindung per WLAN oder Ethernet-Adapter herstellen, können Sie die entsprechenden Einstellungen für ein sicheres Surfvergnügen konfigurieren. Ihnen stehen die folgenden Optionen zur Auswahl:

- **Dynamisch** – Legt den Netzwerktyp automatisch anhand des Profils des Netzwerks fest, mit dem Sie verbunden sind (Heim/Büro oder öffentlich). Tritt dies ein, werden nur die Firewall-Regeln angewendet, die für diesen Netzwerktyp bzw. für alle Netzwerktypen konfiguriert wurden.

- **Heim/Büro** – Der Netzwerktyp wird immer als Heim/Büro festgelegt, unabhängig von Profil des Netzwerks, mit dem Sie verbunden sind. Tritt dies ein, werden nur die Firewall-Regeln angewendet, die für Heim/Büro bzw. für alle Netzwerktypen konfiguriert wurden.
- **Öffentlich** – Der Netzwerktyp wird immer als öffentlich festgelegt, unabhängig von Profil des Netzwerks, mit dem Sie verbunden sind. Tritt dies ein, werden nur die Firewall-Regeln angewendet, die für öffentliche Netzwerke bzw. für alle Netzwerktypen konfiguriert wurden.

So konfigurieren Sie Ihre Netzwerkadapter:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **FIREWALL**.
4. Wählen Sie den Reiter **NETZWERKTYP** aus.
5. Wählen Sie die Einstellungen aus, die bei Verbindungen mit den folgenden Adaptern angewendet werden sollen:
   - WLAN
   - Ethernet

## 4.5.3. Konfigurieren der erweiterten Einstellungen

So können Sie die erweiterten Firewall-Einstellungen konfigurieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **FIREWALL**.
4. Wechseln Sie zum Reiter **EINSTELLUNGEN**.

Die folgenden Funktionen können konfiguriert werden:

- **Port-Scans im Netzwerk blockieren** - Erkennt und blockiert Versuche offene Ports zu finden.

Portscans werden von Hackern verwendet, um herauszufinden, welche Ports auf Ihrem Computer geöffnet sind. Wenn Sie dann einen unsicheren Port finden, können Sie in Ihren Computer eindringen.

- **Paranoiamodus** - Sie werden über jeden Versuch einer Anwendung, eine Internetverbindung aufzubauen, benachrichtigt. Wählen Sie **Zulassen** oder **Blockieren** aus. Bei Aktivierung des Paranoiamodus werden der Autopilot und die Profile-Funktionen automatisch deaktiviert. Der Paranoiamodus kann während des **Akkubetriebs** verwendet werden.
- **Tarnkappe** - Ob Sie von anderen Computern entdeckt werden können. Klicken Sie auf **Tarneinstellungen bearbeiten**, um festzulegen, wann Ihr Computer für andere Computer sichtbar sein soll und wann nicht.
- **Standardmäßiges Anwendungsverhalten** - Erlaubt, dass Bitdefender automatische Einstellungen auf Anwendungen ohne festgelegte Regel anwendet. Klicken Sie auf **Standardregeln bearbeiten**, um festzulegen, ob automatische Einstellungen angewendet werden sollen oder nicht.
  - Automatisch - Der Anwendungszugriff wird anhand der automatischen Firewall-Regeln und der benutzerdefinierten Regeln zugelassen oder verweigert.
  - Zulassen - Anwendungen ohne festgelegte Firewall-Regeln werden automatisch zugelassen.
  - Blockieren - Anwendungen ohne festgelegte Firewall-Regeln werden automatisch blockiert.

## 4.6. Schwachstellen

Ein wichtiger Schritt für den Schutz Ihres Computers gegen Angriffe und schädliche Anwendungen besteht darin, das Betriebssystem und regelmäßig genutzte Programme stets auf dem neusten Stand zu halten. Darüber hinaus müssen für jedes Windows-Benutzerkonto und die genutzten WLAN-Netzwerke sichere Passwörter vergeben werden, um zu verhindern, dass ein nicht autorisierter physikalischer Zugriff auf Ihren Computer erfolgt.

Bitdefender überprüft Ihr System automatisch auf Schwachstellen und informiert Sie über diese. Dabei sucht es nach:

- veraltete Apps auf Ihrem Computer.
- fehlende Windows Updates.
- Schwache Windows Benutzerkonten Passwörter.

- ungesicherte WLAN-Netzwerke und Router.

Bitdefender bietet Ihnen zwei einfache Möglichkeiten, die Schwachstellen Ihres Systems zu beheben:

- Sie können Ihr System nach Schwachstellen durchsuchen und diese Schritt für Schritt mit dem **Schwachstellen-Scan** beheben.
- Mithilfe der automatischen Schwachstellenüberwachung können Sie im Benachrichtigungen-Fenster erkannte Schwachstellen überprüfen und beheben.

Sie sollten Ihr System alle ein bis zwei Wochen nach Schwachstellen durchsuchen und diese beheben.

### 4.6.1. Scannen des Computers nach Schwachstellen

So können Sie Systemschwachstellen mit dem Schwachstellen-Scan beheben:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf die Schaltfläche **Schwachstellen-Scan**.
3. Bitte warten Sie, bis Bitdefender die Schwachstellenprüfung beendet hat. Klicken Sie unten im Fenster auf **Überspringen**, um den Scan-Vorgang zu beenden.

   - **Kritische Windows-Updates**

     Klicken Sie auf **Details anzeigen**, um die Liste aller wichtigen Windows-Updates anzuzeigen, die nicht auf Ihrem Computer installiert sind.

     Um die Installation der gewählten Updates zu starten, klicken Sie auf **Updates installieren**. Bitte beachten Sie, dass die Installation der Updates einige Zeit in Anspruch nehmen kann und dass manche Updates einen Neustart erfordern, um die Installation abzuschließen. Falls nötig starten Sie das System sobald es Ihnen möglich ist neu.

   - **Anwendungsupdates**

     Wenn eine Anwendung nicht auf dem neusten Stand ist, klicken Sie auf **Neue Version herunterladen**, um die aktuellste Version herunterzuladen.

Klicken Sie auf **Details anzeigen**, um Informationen zu der Anwendung anzuzeigen, die aktualisiert werden muss.

- **Unsichere Passwörter für Windows-Benutzerkonten**

  Sie können die Liste der auf Ihrem Computer konfigurierten Windows-Benutzerkonten sehen und die Sicherheit, die das jeweilige Passwort bietet.

  Klicken Sie auf **Passwortwechsel beim Login**, um ein neues Passwort für Ihr System festzulegen.

  Klicken Sie auf **Details anzeigen**, um unsichere Passwörter zu ändern. Sie können den jeweiligen Benutzer auffordern, das Passwort bei der nächsten Anmeldung zu ändern oder das Passwort sofort selbst ändern. Verwenden Sie für ein sicheres Passwort eine Kombination aus Groß- und Kleinschreibung, Zahlen und Sonderzeichen (z.B. #, $ or @).

- **schwache WLAN-Netzwerke**

  Klicken Sie auf **Details anzeigen**, um weitere Informationen zu dem Drahtlosnetzwerk zu erhalten, mit dem Sie aktuell verbunden sind. Falls Sie ein sichereres Passwort für Ihr Heimnetzwerk festlegen sollen, klicken Sie auf den entsprechenden Link.

  Falls weitere Empfehlungen vorliegen, können Sie den Anweisungen folgen, um Ihr Heimnetzwerk vor Hackern zu schützen.

Oben rechts im Fenster können Sie die Ergebnisse entsprechend Ihrer Anforderungen filtern.

## 4.6.2. Automatische Schwachstellensuche

Bitdefender scannt Ihr System im Hintergrund regelmäßig nach Schwachstellen und erfasst alle erkannten Probleme im Fenster Benachrichtigungen.

So können Sie erkannte Probleme prüfen und beheben:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wählen Sie unter dem Reiter **Alle** die Benachrichtigung bezüglich des neuesten Schwachstellen-Scans aus.

3. Sie erhalten detaillierte Informationen zu den erkannten Systemschwachstellen. Abhängig vom Problem, um eine spezifische Schwachstelle zu beheben, gehen Sie folgendermaßen vor:
   - Falls Windows-Updates verfügbar sind, klicken Sie auf **INSTALLIEREN**.
   - Klicken Sie auf **AKTIVIEREN**, falls automatische Windows-Updates deaktiviert wurden.
   - Falls eine Anwendung nicht mehr auf dem neuesten Stand ist, klicken Sie auf **JETZT AKTUALISIEREN**, um einen Link zur Website des Anbieters zu finden, von der aus Sie die neueste Version der Anwendung installieren können.
   - Wenn ein Windows-Benutzerkonto mit einem unsicheren Passwort gesichert ist, klicken Sie auf **PASSWORT ÄNDERN**, um den Benutzer dazu zu zwingen, das Passwort bei der nächsten Anmeldung zu ändern oder es selbst zu ändern. Verwenden Sie für ein sicheres Passwort eine Kombination aus Groß- und Kleinschreibung, Zahlen und Sonderzeichen (z.B. #, $ or @).
   - Sollte die Autorun-Funktion in Windows aktiviert sein, klicken Sie auf **BEHEBEN**, um sie zu deaktivieren.
   - Falls für den von Ihnen konfigurierten Router ein unsicheres Passwort vergeben wurde, klicken Sie auf **PASSWORT ÄNDERN**, um auf seine Benutzeroberfläche zuzugreifen und das Passwort entsprechend anzupassen.
   - Falls das Netzwerk, mit dem Sie verbunden sind, Schwachstellen aufweist, die Ihr System gefährden könnten, klicken Sie auf **WLAN-EINSTELLUNGEN ÄNDERN**.

So können Sie die Einstellungen für die Schwachstellensuche konfigurieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **SCHWACHSTELLE** auf den EIN/AUS-Schalter.

> **Wichtig**
> Um automatisch über System- oder Anwendungsschwachstellen benachrichtigt zu werden, lassen Sie die Option **Schwachstellen** aktiviert.

4. Nutzen Sie die entsprechenden Schalter, um die Systemschwachstellen auszuwählen, die Sie regelmäßig überprüfen möchten.

   **Kritische Windows-Updates**
   Überprüfen Sie, ob die neuesten kritischen Microsoft-Sicherheits-Updates auf Ihrem Windows-Betriebssystem installiert sind.

   **Anwendungsupdates**
   Prüfen Sie, ob die auf Ihren System installierten Anwendungen aktuell sind. Veraltete Anwendungen können von schädlicher Software ausgenutzt werden und Ihren PC so anfällig für Angriffe von außen machen.

   **Unsichere Passwörter**
   Überprüfen Sie, ob die Passwörter Ihrer Windows-Benutzerkonten und Router leicht zu erraten sind oder nicht. Passwörter, die schwer zu erraten sind (starke Passwörter), mache es sehr schwierig für Hacker, in Ihr System einzudringen. Ein starkes Passwort sollte aus Klein- und Großbuchstaben, Ziffern und Sonderzeichen (z.B. #, $ oder @) bestehen.

   **Medien-Autostart**
   Überprüfen Sie den Status der Windows-Autorun-Funktion. Mit dieser Funktion lassen sich Anwendungen automatisch direkt von CD, DVD, USB-Stick oder anderen externen Speichermedien starten.

   Manche Bedrohungsarten verbreiten sich über den Autostart von Wechselmedien auf Ihrem PC. Aus diesem Grund sollten Sie diese Windows-Funktion deaktivieren.

   **WLAN-Sicherheitsberater-Benachrichtigungen**
   Prüfen Sie, ob das Heim-WLAN, mit dem Sie verbunden sind, sicher ist und ob Schwachstellen vorliegen. Überprüfen Sie zudem, ob das Passwort für Ihren Heim-Router ausreichend sicher ist und wie Sie es bei Bedarf sicherer machen können.

   Die Mehrzahl der ungeschützten Drahtlosnetzwerke sind nicht sicher und erlauben Hackern ohne Weiteres, an Ihren privaten Aktivitäten teilzuhaben.

**Beachten Sie**
Wenn Sie die Überwachung einer bestimmten Schwachstelle deaktivieren, werden damit zusammenhängende Probleme nicht mehr im Benachrichtigungsfenster erfasst.

## 4.6.3. WLAN-Sicherheitsberater

Egal ob unterwegs, bei der Arbeit in einem Café oder beim Warten am Flughafen: Oftmals ist es am bequemsten, sich mit einem öffentlichen WLAN zu verbinden, um Zahlungen anzuweisen, E-Mails abzurufen oder einen schnellen Blick in soziale Netzwerke zu werfen. Aber hier können auch Datenjäger lauern, die nur darauf warten, dass Ihre persönlichen Daten durch das Netzwerk wandern.

Persönliche Daten wie Ihre Passwörter und Benutzernamen, die Sie zur Anmeldung bei Ihren Online-Konten für E-Mail, Bankgeschäfte, und Social Media nutzen, aber auch die Nachrichten die Sie verschicken.

Öffentliche WLAN-Netzwerke sind in aller Regel nicht besonders sicher, da sie bei der Anmeldung kein Passwort anfordern. Und falls doch, wird dieses Passwort allen zur Verfügung gestellt, die sich dort anmelden möchten. Darüber hinaus könnten Sie in betrügerischer Absicht oder als Honeypot eingerichtet worden sein und sind damit ein Ziel für Cyberkriminelle.

Um Sie vor den gefahren ungesicherter oder unverschlüsselter öffentlicher WLAN-Hotspots zu schützen, prüft der Bitdefender-WLAN-Sicherheitsberater, wie sicher ein WLAN-Netzwerk ist und schlägt bei Bedarf die Nutzung vonBitdefender VPN vor.

Der Bitdefender-WLAN-Sicherheitsberater liefert Informationen zu:

- Heim-WLAN-Netzwerken
- Öffentlichen WLAN-Netzwerken

### Aktivieren und Deaktivieren der Benachrichtigungen des WLAN-Sicherheitsberaters

So können Sie die Benachrichtigungen des WLAN-Sicherheitsberaters aktivieren oder deaktivieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.

2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das ⚙ -Symbol unten rechts im Bereich **SCHWACHSTELLE**.
4. Klicken Sie im Fenster **EINSTELLUNGEN** auf den entsprechenden EIN/AUS-Schalter.

## Konfiguration Ihres Heim-WLANs

So beginnen Sie mit der Konfiguration Ihres Heimnetzwerks:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das Ⓑ -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **SCHWACHSTELLE** auf **WLAN-Sicherheitsberater**.
4. Klicken Sie im Reiter **HEIM-WLAN** auf **HEIM-WLAN AUSWÄHLEN**.

   Eine Liste der bisher genutzten WLAN-Netzwerke wird angezeigt.
5. Bewegen Sie den Mauszeiger auf Ihr Heim-WLAN und klicken Sie auf **AUSWÄHLEN**.

Falls Ihr Heimnetzwerk als ungesichert oder unsicher eingestuft wurde, werden Konfigurationsempfehlungen zur Verbesserung der Sicherheit eingeblendet.

Um ein WLAN-Netzwerk zu entfernen, das Sie als Heimnetzwerk festgelegt haben, klicken Sie auf **ENTFERNEN**.

## Öffentliches WLAN

Bei Verbindungen mit einem ungesicherten oder unsicheren WLAN-Netzwerk wird das Öffentliche WiFi-Profil aktiviert. Bei Aktivierung dieses Profils werden von Bitdefender Total Security 2018 automatisch die folgenden Programmeinstellungen vorgenommen:

- Die Erweiterte Gefahrenabwehr ist aktiviert
- Die Bitdefender-Firewall ist aktiviert und die folgenden Einstellungen werden auf Ihren Drahtlosadapter angewandt.
  - Tarnkappe - AKTIVIERT
  - Netzwerktyp - Öffentlich
- Die folgenden Einstellungen des Internet-Schutzes werden aktiviert:

- SSL scannen
- Schutz gegen Betrug
- Schutz vor Phishing-Attacken

- Eine Schaltfläche zum Öffnen von Bitdefender Safepay™ wird angezeigt. In diesem Fall wird der Hotspot-Schutz für ungesicherte Netzwerke standardmäßig aktiviert.

## Abrufen von Informationen zu WLAN-Netzwerken

So können Sie Informationen zu den WLAN-Netzwerken abrufen, zu denen Sie regelmäßig Verbindungen herstellen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **SCHWACHSTELLE** auf **WLAN-Sicherheitsberater**.
4. Wählen Sie je nach benötigter Information den Reiter **HEIM-WLAN** oder **ÖFFENTLICHES WLAN** aus.
5. Klicken Sie neben dem Netzwerk, über das Sie sich informieren möchten, auf **Details anzeigen**.

Es gibt drei Arten von WLAN-Netzwerken, die nach ihrer Wichtigkeit sortiert werden. Diese werden durch verschiedene Symbole unterschieden:

**WLAN ist unsicher** - Zeigt an, dass das Netzwerk geringe Sicherheit bietet. Das heißt, dass mit einer Nutzung ein hohes Risiko einhergeht und ohne zusätzlichen Schutz keine Zahlungen vorgenommen oder Bankkonten eingesehen werden sollten. In solchen Fällen empfehlen wir Ihnen die Nutzung von Bitdefender Safepay™ mit aktiviertem Hotspot-Schutz für ungesicherte Netzwerke.

**WLAN ist unsicher** - Zeigt an, dass das Netzwerk mittlere Sicherheit bietet. Das heißt, dass Schwachstellen vorliegen könnten und ohne zusätzlichen Schutz keine Zahlungen vorgenommen oder Bankkonten eingesehen werden sollten. In solchen Fällen empfehlen wir Ihnen die Nutzung von Bitdefender Safepay™ mit aktiviertem Hotspot-Schutz für ungesicherte Netzwerke.

**WLAN ist sicher** - Zeigt an, dass das verwendete Netzwerk sicher ist. In diesem Fall können Sie bei Ihren Online-Aktivitäten auch sensible Daten verwenden.

Mit einem Klick auf **Details anzeigen ...** im Bereich der einzelnen Netzwerke werden die folgenden Details angezeigt:

- **Gesichert** - Hier sehen Sie, ob das ausgewählte Netzwerk sicher ist oder nicht. Unverschlüsselte Netzwerke können eine Gefahr für Ihre Daten darstellen.
- **Verschlüsselungstyp** - Hier sehen Sie, welcher Verschlüsselungstyp von dem ausgewählten Netzwerk verwendet wird. Manche Verschlüsselungstypen sind unter Umständen nicht sicher. Wir möchten Ihnen daher nachdrücklich empfehlen, die Informationen über den Verschlüsselungstyp einzusehen, um sicherzustellen, dass Sie sicher im Netz surfen.
- **Kanal/Frequenz** - Hier können Sie die Kanalfrequenz des ausgewählten Netzwerks einsehen.
- **Passwortsicherheit** - Hier sehen Sie, wie sicher das Passwort ist. Bitte beachten Sie, dass Netzwerke mit unsicheren Passwörtern für Cyberkriminelle besonders attraktiv sind.
- **Art der Anmeldung** - Hier können Sie sehen, ob das ausgewählte Netzwerk mit einem Passwort geschützt ist oder nicht. Wir empfehlen Ihnen dringend, ausschließlich Verbindungen mit Netzwerken herzustellen, die mit sicheren Passwörtern geschützt sind.
- **Authentifizierungstyp** - Hier sehen Sie, welcher Authentifizierungstyp von dem ausgewählten Netzwerk verwendet wird.

Lassen Sie die Option **Benachrichtigen** aktiviert, um benachrichtigt zu werden, wenn Ihr System eine Verbindung mit diesem Netzwerk aufbaut.

## 4.7. Webcam-Schutz

Die Tatsache, dass Hacker Ihre Webcam nutzen könnten, um Sie auszuspionieren, ist längst nichts Neues mehr. Lösungsansätze wie das Widerrufen von Anwendungsberechtigungen, die Deaktivierung der integrierten Kamera und das Abdecken der Linse erweisen sich als eher unpraktisch. Um weitere Zugriffsversuche zu unterbinden, überwacht der Bitdefender-Webcam-Schutz durchgehend alle Apps, die versuchen, auf Ihre Webcam zuzugreifen, und blockiert alle Apps, die nicht als vertrauenswürdig eingestuft wurden.

Als zusätzliche Sicherheitsmaßnahme erhalten Sie eine Benachrichtigung über jeden Versuch einer nicht vertrauenswürdigen App, auf Ihre Kamera zuzugreifen, auch dann, wenn der Autopilot aktiviert ist.

## Aktivieren und Deaktivieren des Webcam-Schutzes

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **WEBCAM-SCHUTZ** auf den EIN/AUS-Schalter.

## Konfigurieren des Webcam-Schutzes

So legen Sie fest, welche Regeln angewendet werden sollen, wenn eine App versucht, auf Ihre Kamera zuzugreifen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **WEBCAM-SCHUTZ**.

**Blockierungsregeln für Anwendungen**

- **Jeglichen Zugriff auf die Webcam blockieren** - Der Zugriff auf Ihre Webcam wird für alle Anwendungen unterbunden.
- **Webcam-Zugriff für Browser blockieren** - Der Zugriff auf Ihre Webcam wird für alle Browser mit Ausnahme von Internet Explorer und Microsoft Edge unterbunden. Da alle Apps aus dem Windows Store grundsätzlich in einem einzigen Prozess ausgeführt werden, können Internet Explorer und Microsoft Edge von Bitdefender nicht als Web-Browser identifiziert werden, und sind folglich von dieser Einstellung ausgeschlossen.
- **Webcam-Zugriff für Anwendungen anhand der Bitdefender-Benutzerauswahl festlegen** - Wird eine beliebte App von der Mehrzahl der Bitdefender-Benutzer als harmlos eingestuft, wird der Webcam-Zugriff für diese App automatisch zugelassen. Wird eine beliebte App von der Mehrheit als gefährlich eingestuft, wird der Zugriff für diese App automatisch blockiert.

Sie werden benachrichtigt, sobald eine Ihrer installierten Apps von der Mehrzahl der Bitdefender-Benutzer als blockiert gelistet wurde, auch dann, wenn der Autopilot aktiviert ist.

**Nachrichten**

- **Benachrichtigen, wenn zugelassene Anwendungen eine Webcam-Verbindung herstellen** - Sie werden benachrichtigt, sobald eine zugelassene App auf Ihre Webcam zugreift, auch dann, wenn der Autopilot aktiviert ist.

## Hinzufügen von Apps zur Liste für den Webcam-Schutz

Zugriffsversuche von Apps werden automatisch erkannt. Abhängig von App-Verhalten und der Auswahl anderer Benutzer, wird der Zugriff zugelassen oder verweigert. Sie können darüber hinaus auch selbst festlegen, welche Aktionen ausgeführt werden soll, indem Sie folgendermaßen vorgehen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **WEBCAM-SCHUTZ** auf **Webcam-Zugriff**.
4. Bei der ersten Nutzung des Webcam-Schutzes werden Sie mit der Funktion vertraut gemacht.
5. Klicken Sie auf den gewünschten Link:
   - **Wählen Sie Windows-Store-Apps zum Hinzufügen zur Berechtigungsliste aus** - Eine Liste mit allen gefundenen Windows-Store-Apps wird angezeigt. Aktivieren Sie die Schalter neben den Apps, die Sie zur Liste hinzufügen möchten.
   - **Mit dem Hinzufügen von Anwendungen zur Liste für den Webcam-Zugriff beginnen.** - Navigieren Sie zu der .exe-Datei, die Sie zur Liste hinzufügen möchten, und klicken Sie auf **OK**.

     Klicken Sie auf den Link **Eine neue Anwendung zur Liste hinzufügen**, um weitere Apps hinzuzufügen.

Klicken Sie auf den Schalter Zugriff zugelassen/Zugriff blockiert.

Klicken Sie auf das -Symbol, um anzuzeigen, welche Auswahl die Bitdefender-Benutzer für die ausgewählte App getroffen haben.

In diesem Fenster werden neben dem Zeitpunkt der letzten Aktivität alle Apps angezeigt, die den Zugriff auf Ihre Kamera angefordert haben.

Sie werden unabhängig von der Autopilot-Einstellung benachrichtigt, sobald eine der zugelassenen Apps von den Bitdefender-Benutzern blockiert wurde.

## 4.8. Sichere Dateien

Bei Ransomware handelt es sich um Schadsoftware, die anfällige Systeme infiziert und den Zugriff darauf sperrt. Von den Benutzern wird dann für die Freigabe ihrer Daten ein Lösegeld erpresst. Diese Schadsoftware geht intelligent vor und zeigt Benutzern gefälschte Warnmeldungen an, um sie in Angst zu versetzen und sie dazu zu bringen, das geforderte Geld zu zahlen.

Übertragen werden kann die Infektion durch Spam-Nachrichten, das Herunterladen von Anhängen an oder durch das Aufrufen infizierter Websites und die Installation von schädlichen Apps, ohne dass der Benutzer überhaupt merkt, was auf seinem System vorgeht.

Ransomware kann den Benutzer auf die folgenden Arten aus seinem System aussperren:

- Verschlüsselung sensibler und persönlicher Dateien, die erst nach Zahlung durch das Opfer wieder entschlüsselt werden können.
- Sperren des Bildschirms und Anzeige einer Benachrichtigung, die ebenfalls die Zahlung eines Geldbetrags fordert. In diesen Fällen erfolgt keine Verschlüsselung der Dateien, der Benutzer wird jedoch dennoch gezwungen, die Zahlung vorzunehmen.
- Verhindert die Ausführung von Apps.

Mit Bitdefender Sichere Dateien schützen Sie sich vor Ransomware-Angriffen auf Ihre persönlichen Dateien, so zum Beispiel Ihre Dokumente, Fotos oder Filme.

### Beachten Sie

Erweiterte Gefahrenabwehr und Sichere Dateien bilden zwei Sicherheitsebenen zur Abwehr von Ransomware. Bei der Erweiterten Gefahrenabwehr handelt es sich um eine Funktion, die Ransomware-Angriffe aufhält, bevor Sie kritische Systembereiche erreichen kann. Sichere Dateien sorgt dafür, dass die wichtigen Dateien auf Ihrem Computer nicht verschlüsselt werden können.

### 4.8.1. Aktivieren und Deaktivieren von Sichere Dateien

So können Sie die Sichere Dateien-Funktion aktivieren oder deaktivieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **SICHERE DATEIEN** auf den EIN/AUS-Schalter.

Versucht eine Anwendung nun, auf eine geschützte Datei zuzugreifen, wird ein Bitdefender-Pop-up-Fenster angezeigt. Sie können den Zugriff erlauben oder blockieren.

**Beachten Sie**
Die Funktion Sichere Dateien ist standardmäßig nicht aktiviert.

### 4.8.2. Schützen Sie Ihre persönlichen Dateien vor Ransomware-Angriffen.

So können Sie persönliche Dateien besonders schützen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **SICHERE DATEIEN** auf **Geschützte Ordner**.
4. Beim ersten Aufrufen von Geschützte Ordner werden Sie mit der Funktion vertraut gemacht. Klicken Sie zum Fortfahren auf **WEITERE ORDNER SCHÜTZEN**.
5. Wählen Sie den zu schützenden Ordner aus und klicken Sie auf **OK**.

   Klicken Sie zum Hinzufügen weiterer Ordner auf den Link **Weitere Ordner schützen**. Alternativ dazu können Sie die Ordner auch in dieses Fenster verschieben.

Die Ordner Bilder, Videos, Musik, Desktop und Downloads werden standardmäßig vor Angriffen geschützt. Sofern die entsprechenden Anwendungen auf dem System installiert sind, können auch bei File-Hosting-Diensten wie Box, Dropbox, Google Drive und OneDrive gespeicherte Daten zur geschützten Umgebung hinzugefügt werden.

Um Systembeeinträchtigungen zu vermeiden, sollten Sie nicht mehr als 30 Ordner hinzufügen oder mehrere Dateien in einem Ordner speichern.

**Beachten Sie**
Benutzerdefinierte Ordner können nur für den aktuellen Benutzer geschützt werden. System- und Anwendungsdateien können zu den Ausschlüssen nicht hinzugefügt werden.

### 4.8.3. Konfiguration des App-Zugriffs

Anwendungen, die versuchen, geschützte Dateien zu verändern oder zu löschen, können als potenziell unsicher markiert und zur Liste der blockierten Anwendungen hinzugefügt werden. Falls eine solche Anwendung blockiert wurde und Sie sich sicher sind, dass ihr Verhalten normal ist, können Sie ihre Ausführung wie folgt zulassen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **SICHERE DATEIEN** auf **Anwendungszugriff**.
4. Hier werden alle Anwendungen aufgelistet, die versucht haben, Dateien in Ihren geschützten Ordnern zu verändern. Klicken Sie auf Zulassen und wählen Sie die Anwendung aus, die Sie als sicher einstufen.

Im gleichen Fenster können Sie mit einem Klick auf Blockieren den Ransomware-Schutz für bestimmte Anwendungen deaktivieren.

Klicken Sie auf den Link **Eine neue Anwendung zur Liste hinzufügen**, um neue Anwendungen zur Liste hinzuzufügen.

### 4.8.4. Schutz beim Systemstart

Viele schädliche Apps sind bekanntermaßen darauf ausgelegt, beim Systemstart ausgeführt zu werden, und können einen Computer so ernsthaft beschädigen. Der Bitdefender-Systemstartschutz scannt alle kritischen Systembereiche noch bevor alle Dateien geladen werden, ohne dabei die Systemleistung zu beeinträchtigen.

So können Sie den Schutz beim Systemstart deaktivieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.

2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das ⚙ -Symbol unten rechts im Bereich **SICHERE DATEIEN**.
4. Klicken Sie auf den EIN/AUS-Schalter.

> **Beachten Sie**
> Zu den Ausschlüssen hinzugefügte Anwendungen werden ebenfalls gescannt und entsprechend behandelt.

## 4.9. Verschlüsselung

Die Bitdefender-Dateiverschlüsselung ermöglicht das Erstellen von verschlüsselten, passwortgeschützten logischen Laufwerken (Tresoren) auf Ihrem Computer, in denen Sie sicher Ihre vertraulichen und sensiblen Dokumente speichern können. Auf die Daten, die im Tresor gespeichert sind, können nur die Personen zugreifen, die das Passwort kennen. Die Daten, die in den Tresoren gespeichert sind, können nur von Benutzern aufgerufen werden, die das Passwort kennen.

Mit dem Passwort können Sie einen Tresor öffnen, Daten darin speichern und den Tresor verriegeln, wobei dieser sicher bleibt. Wenn ein Tresor geöffnet ist, können Sie neue Dateien hinzufügen, auf aktuelle Dateien zugreifen oder diese verändern.

Physisch gesehen ist der Tresor eine auf der lokalen Festplatte gespeicherte Datei mit der Endung .bvd. Auch wenn die physischen Dateien, die die tresorgeschützten Laufwerke darstellen, von anderen Betriebssystemen (beispielsweise Linux) aufgerufen werden können, können die darin gespeicherten Informationen nicht gelesen werden, weil sie verschlüsselt sind.

Datentresore können über das Bitdefender-Fenster heraus verwaltet werden oder über die Windows-Kontextmenüs und logischen Laufwerke, die mit dem Tresor verknüpft sind.

### Verwalten der Datentresore

Klicken Sie auf das 👁 -Symbol im linken Seitenbereich der Bitdefender-Benutzeroberfläche, um Ihre Datentresore in Bitdefender zu verwalten.

Alle bereits erstellten Datentresore werden im Bereich **Datentresore** angezeigt.

## Anlegen von Datentresoren

So können Sie einen neuen Tresor anlegen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **DATEIVERSCHLÜSSELUNG** auf **Neuen Datentresor erstellen**.
4. Geben Sie den Namen und den Speicherort der Tresordatei an.
   - Geben Sie Namen der Tresordatei in das entsprechende Feld ein.
   - Klicken Sie auf **Durchsuchen**, wählen Sie den gewünschten Speicherort und speichern Sie die Tresordatei unter dem gewünschten Namen.
5. Wählen Sie aus dem entsprechenden Menü den Laufwerksbuchstaben aus. Wenn Sie einen Datentresor öffnen, wird ein virtuelles Laufwerk mit dem gewählten Laufwerksbuchstaben unter Arbeitsplatz erscheinen.
6. Sie können die Standardgröße (100 MB) des Datentresors über die Pfeiltasten im Drehfeld **Tresorgröße (MD)** ändern.
7. Geben Sie das gewünschte Passwort für den Tresor in die Felder **Passwort** und **Passwort bestätigen** ein. Ihr Passwort muss mindestens 8 Zeichen lang sein. Jeder, der den Datentresor öffnen und auf die Dateien zugreifen möchte, muss zuerst das Passwort angeben.
8. Klicken Sie auf **Erstellen**.

Bitdefender wird Sie unmittelbar über das Ergebnis der Operation informieren. Ist ein Fehler aufgetreten, können Sie die Fehlermeldung verwenden, um die Ursache des Problems zu finden.

Um einen neuen Tresor noch schneller zu erstellen, rufen Sie im Desktop-Bereich oder innerhalb eines Ordners per Rechtsklick das Kontextmenü auf und wählen Sie **Bitdefender** > **Bitdefender -Datentresor** und anschließend **Tresor erstellen** aus.

### Beachten Sie

Es kann praktisch sein, alle Datentresore am gleichen Ort zu speichern. Dann sind sie einfacher zu finden.

## Importieren eines Datentresors

So importieren Sie einen lokal gespeicherten Datentresor:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie unter **DATEIVERSCHLÜSSELUNG** auf **Tresor importieren**.
4. Suchen Sie den Datentresor und markieren Sie ihn (die Datei mit der Endung .bvd).
5. Klicken Sie auf **Öffnen**.

## Öffnen eines Datentresors

Um auf die Dateien in einem Datentresor zugreifen und mit ihnen arbeiten zu können, muss der Datentresor geöffnet werden. Wenn Sie einen Datentresor öffnen, erscheint ein virtuelles Laufwerk unter Arbeitsplatz. Dieses Laufwerk hat den Laufwerksbuchstaben, der dem Datentresor zugewiesen wurde.

So können Sie einen Datentresor öffnen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.

   Alle bereits erstellten Datentresore werden im Bereich **Datentresore** angezeigt.
2. Klicken Sie auf den Link **Tresore anzeigen** und wählen Sie den Datentresor aus, der geöffnet werden soll.
3. Klicken Sie auf **Entsperren** und geben Sie das benötigte Passwort ein.
4. Klicken Sie auf **OK** und danach auf **Öffnen**, um Ihren Datentresor zu öffnen.

Bitdefender wird Sie unmittelbar über das Ergebnis der Operation informieren. Ist ein Fehler aufgetreten, verwenden Sie die Fehlermeldung, um die Ursache des Fehlers zu finden.

Ein Tresor lässt sich noch schneller öffnen, indem Sie den Ordner mit der .bvd-Datei öffnen, die für den jeweiligen Datentresor steht. Rechtsklicken Sie auf die Datei, bewegen Sie den Mauszeiger auf **Bitdefender-Datentresor** und

wählen Sie **Öffnen**. Geben Sie das benötigte Passwort ein und klicken Sie auf **OK**.

## Dateien zu einem Datentresor hinzufügen

Bevor Sie dem Datentresor Dateien oder Verzeichnisse hinzufügen können, müssen Sie den Tresor öffnen.

So können Sie neue Dateien zu Ihrem Datentresor hinzufügen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **DATEIVERSCHLÜSSELUNG**.
4. Wählen Sie im Fenster **Meine Tresore** die Tresore aus, die Sie öffnen möchten.
5. Klicken Sie auf **Entsperren** und geben Sie das benötigte Passwort ein.
6. Klicken Sie auf **Öffnen**, um Ihren Tresor zu öffnen.
7. Das Hinzufügen von Dateien und Ordnern erfolgt so, wie Sie es aus Windows bereits gewohnt sind (so z. B. mit Kopieren und Einfügen).

Dateien lassen sich noch schneller zu einem Datentresor hinzufügen, indem Sie mit der rechten Maustaste auf die Datei oder den Ordner klicken, den Sie in den Datentresor kopieren möchten, den Mauszeiger auf **Bitdefender-Datentresor** bewegen und auf **Dem Datentresor hinzufügen** klicken.

- Wenn nur ein Datentresor geöffnet ist, wird die Datei oder das Verzeichnis direkt in diesen kopiert.
- Wenn mehrere Tresore geöffnet sind, werden Sie aufgefordert auszuwählen, in welchen Tresor das Objekt kopiert werden soll. Wählen Sie aus dem Menu passend zum gewünschten Tresor den Laufwerksbuchstaben, und klicken Sie auf **OK** um das Objekt zu kopieren.

## Verriegeln von Datentresoren

Wenn Sie mit Ihrer Arbeit im Datentresor fertig sind, müssen Sie diesen verriegeln, um Ihre Daten zu schützen. Durch das Verriegeln des Tresors

verschwindet das entsprechende virtuelle Laufwerk aus dem Arbeitsplatz. Damit ist der Zugriff auf die im Tresor gespeicherten Daten vollständig blockiert.

So können Sie einen Datentresor sperren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie im Bereich **Datentresore** auf **Tresore anzeigen**.
3. Wählen Sie im Fenster **Meine Tresore** die Tresore aus, die Sie sperren möchten.
4. Klicken Sie auf **Sperren**.

Bitdefender wird Sie unmittelbar über das Ergebnis der Operation informieren. Ist ein Fehler aufgetreten, können Sie die Fehlermeldung verwenden, um die Ursache des Problems zu finden.

Um einen Tresor noch schneller zu sperren, klicken Sie mit der rechten Maustaste auf die .bvd-Datei, die für den Tresor steht, bewegen Sie den Mauszeiger auf **Bitdefender-Datentresor** und klicken Sie auf **Sperren**.

## Dateien aus einem Datentresor entfernen

Um Dateien oder Verzeichnisse aus dem Datentresor zu entfernen, muss der Datentresor geöffnet sein. So können Sie Dateien oder Ordner aus einem Tresor entfernen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **DATEIVERSCHLÜSSELUNG**.
4. Wählen Sie im Fenster **Meine Tresore** den Tresor aus, aus dem Sie Dateien entfernen möchten.
5. Klicken Sie auf **Entsperren**, falls dieser gesperrt ist.
6. Klicken Sie auf **Öffnen**.

Entfernen Sie Dateien oder Verzeichnisse wie Sie es normalerweise auch in Windows tun (z.B. rechtsklicken Sie auf die Datei, die Sie löschen möchten und wählen sie **Löschen** aus).

## Ändern des Tresorpassworts

Das Passwort schützt den Inhalt des Datentresors vor unberechtigten Zugriffen. Ausschließlich Benutzer, die das Passwort kennen, können den Datentresor öffnen und auf die darin abgelegten Dokumente und Daten zugreifen.

Der Datentresor muss verschlossen sein, bevor das Passwort geändert werden kann. So können Sie das Passwort eines Tresors ändern:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **DATEIVERSCHLÜSSELUNG**.
4. Wählen Sie im Fenster **MEINE TRESORE** den Tresor aus, für den Sie das Passwort ändern möchten.
5. Klicken Sie auf die Schaltfläche **Einstellungen**.
6. Geben Sie das aktuelle Passwort des Datentresors in das Feld **Altes Passwort** ein.
7. Geben Sie das neue Passwort des Datentresors in die Felder **Neues Passwort** und **Neues Passwort bestätigen** ein.

> **Beachten Sie**
> Ihr Passwort muss mindestens 8 Zeichen lang sein. Verwenden Sie für ein sicheres Passwort eine Kombination aus Groß- und Kleinschreibung, Zahlen und Sonderzeichen (z.B. #, $ or @).

Bitdefender wird Sie unmittelbar über das Ergebnis der Operation informieren. Ist ein Fehler aufgetreten, können Sie die Fehlermeldung verwenden, um die Ursache des Problems zu finden.

Sie können ein Tresorpasswort sogar noch schneller ändern, indem Sie den Ordner mit der .bvd-Datei öffnen, die für den jeweiligen Datentresor steht.

Rechtsklicken Sie auf die Datei, bewegen Sie den Mauszeiger auf **Bitdefender-Datentresor** und wählen Sie **Tresor-Passwort ändern**.

## 4.10. Passwortmanager-Schutz für Ihre Anmeldedaten

Wir nutzen unsere Computer, um im Internet einzukaufen, unsere Rechnungen zu bezahlen, soziale Netzwerke zu besuchen oder Sofortnachrichten zu verschicken.

Aber wie jeder weiß, kann es manchmal schwer sein, sich alle Passwörter zu merken!

Und wenn wir bei Surfen im Internet nicht vorsichtig sind, können wir unsere privaten Daten wie E-Mail-Adresse, Chat-Name oder Kreditkarteninformationen ungewollt preisgeben.

Passwörter und persönliche Daten aufzuschreiben oder auf dem Computer zu speichern, kann gefährlich sein, weil sie dort nicht vor Unbefugten sicher sind, die es auf diese Informationen abgesehen haben. Und es ist eine echte Herausforderung, sich jedes einzelne Passwort zu merken, das Sie für Ihre Online-Konten und Lieblingsseiten festgelegt haben.

Gibt es also eine Möglichkeit, unsere Passwörter zu aufzubewahren, dass wir jederzeit darauf zugreifen können? Und können wir sicher sein, dass unsere Passwörter auch geheim bleiben?

Der Passwortmanager hilft Ihnen, nie wieder ein Passwort zu vergessen. Zudem schützt er Ihre Privatsphäre und garantiert ein sicheres Internet-Vergnügen.

Durch die Verwendung eines Master-Passworts für den Zugriff auf Ihre Anmeldedaten schützt der Passwortmanager Ihre Passwörter zuverlässig in einer Geldbörse.

Um Ihre Online-Aktivitäten optimal abzusichern, ist der Passwortmanager mit Bitdefender Safepay™ integriert und bietet eine einheitliche Lösung für den Schutz vor den vielen Bedrohungen, denen Ihre Daten ausgesetzt sind.

Mit dem Passwortmanager können die folgenden privaten Daten geschützt werden:

- Persönliche Daten wie zum Beispiel E-Mail-Adressen oder Telefonnummern
- Anmeldeinformationen für verschiedene Websites
- Kontonummern oder Kreditkarteninformationen

- Informationen zu E-Mail-Konten
- Passwort für die Apps
- WLAN-Passwörter

## Neue Geldbörsen-Datenbank erstellen

In der Bitdefender-Geldbörse können Sie Ihre persönlichen Daten speichern. Um bequemer zu surfen, müssen Sie eine Geldbörse-Datenbank erstellen. Gehen Sie dazu wie folgt vor:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **GELDBÖRSE** auf **Neue Geldbörse anlegen**.
4. Klicken Sie auf **Neu anlegen**.
5. Geben Sie die Daten in die entsprechenden Felder ein.
   - Geldbörsenbezeichnung - Geben Sie Ihrer Geldbörse-Datenbank einen eindeutigen Namen
   - Master-Passwort - Geben Sie ein Passwort für Ihre Geldbörse ein.
   - Passwort wiederholen - Wiederholen Sie das angegebene Passwort.
   - Hinweis - Geben Sie einen Passworthinweis ein.
6. Klicken Sie auf **Fortfahren**.
7. An diesem Punkt können Sie angeben, ob Sie Ihre Informationen in der Cloud speichern möchten. Wenn Sie Ja auswählen, werden Ihre Bankdaten auch weiterhin lokal auf Ihrem Gerät gespeichert werden. Wählen Sie die gewünschte Option aus und klicken Sie auf **Fortfahren**.
8. Wählen Sie den Web-Browser aus, aus dem Sie die Anmeldedaten importieren möchten.
9. Klicken Sie auf **Fertigstellen**.

## Bestehende Datenbank importieren

So importieren Sie eine lokal gespeicherte Geldbörse-Datenbank:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **GELDBÖRSE** auf **Neue Geldbörse anlegen**.
4. Klicken Sie auf **Aus Ziel**.
5. Suchen Sie den Speicherort, auf dem Sie die Geldbörse-Datenbank speichern möchten, und vergeben Sie einen Namen für die Datenbank.
6. Klicken Sie auf **Öffnen**.
7. Geben Sie Ihrer Geldbörse einen Namen und geben Sie das Passwort ein, das bei der Erstellung festgelegt wurde.
8. Klicken Sie auf **Importieren**.
9. Markieren Sie die Programme, von denen die Geldbörse Zugangsdaten importieren soll und klicken Sie dann auf **Beenden**.

## Die Geldbörse-Datenbank exportieren

So können Sie Ihre Geldbörse-Datenbank exportieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **GELDBÖRSE** auf **Meine Geldbörsen**.
4. Klicken Sie auf das -Symbol der gewünschten Geldbörse und klicken Sie dann auf **Export**.
5. Suchen Sie Ihre Geldbörse-Datenbank und markieren Sie sie (die Datei mit der Endung .db).
6. Klicken Sie auf **Speichern**.

### Beachten Sie

Die Geldbörse muss geöffnet sein, damit die Option für den **Export** verfügbar ist.
Sollte die Geldbörse, die Sie exportieren möchten, gesperrt sein, klicken Sie auf die Schaltfläche **GELDBÖRSE AKTIVIEREN** und geben Sie anschließend das bei der Erstellung festgelegte Passwort ein.

## Synchronisieren Ihrer Geldbörsen in der Cloud

So können Sie die Synchronisierung der Geldbörse in die Cloud aktivieren oder deaktivieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **GELDBÖRSE** auf **Meine Geldbörsen**.
4. Klicken Sie auf das -Symbol der gewünschten Geldbörse und dann auf **Einstellungen**.
5. Ein neues Fenster wird angezeigt. Wählen Sie die gewünschte Option aus und klicken Sie auf **Speichern**.

### Beachten Sie

Die Geldbörse muss geöffnet sein, damit die Option für den **Export** verfügbar ist.
Sollte die Geldbörse, die Sie synchronisieren möchten, gesperrt sein, klicken Sie auf die Schaltfläche **GELDBÖRSE AKTIVIEREN** und geben Sie anschließend das bei der Erstellung festgelegte Passwort ein.

## Geldbörse-Anmeldedaten verwalten

So können Sie Ihre Passwörter verwalten:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **GELDBÖRSE** auf **Meine Geldbörsen**.
4. Wählen Sie die gewünschte Geldbörse-Datenbank im Fenster **MEINE GELDBÖRSEN** aus und klicken Sie auf **GELDBÖRSE AKTIVIEREN**.
5. Geben Sie das Master-Passwort ein und klicken Sie auf **OK**.

Ein neues Fenster wird angezeigt. Wählen Sie im Fenster oben die gewünschte Kategorie aus:

- Identität
- Webseiten

- Online-Banking
- EMails
- Apps
- WLAN

## Hinzufügen/Bearbeiten von Anmeldedaten

- Um ein neues Passwort hinzuzufügen, wählen Sie oben die entsprechende Kategorie aus, klicken Sie auf **+ Objekt hinzufügen**, geben Sie die Informationen in den entsprechenden Feldern ein und klicken Sie auf Speichern.
- Um ein Objekt aus der Liste zu bearbeiten, klicken Sie auf die **Bearbeiten**-Schaltfläche.
- Um einen Eintrag zu entfernen, wählen Sie ihn aus und klicken Sie auf **Löschen**.

## Aktivieren oder Deaktivieren des Passwortmanager-Schutzes

So können Sie den Passwortmanager aktivieren oder deaktivieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **GELDBÖRSE** auf den EIN/AUS-Schalter.

## Verwaltung der Passwortmanager-Einstellungen

So können Sie das Master-Passwort detailliert konfigurieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **GELDBÖRSE**.
4. Wechseln Sie zum Reiter **SICHERHEITSEINSTELLUNG**.

Die folgenden Optionen sind verfügbar:

- **Nach meinem Master-Passwort fragen, wenn ich mich an meinem PC anmelde** - Sie werden aufgefordert, Ihr Master-Passwort beim Zugriff auf den Computer anzugeben.
- **Nach meinem Master-Passwort fragen, wenn ich meine Browser und Anwendungen öffne** - Sie werden aufgefordert, Ihr Master-Passwort beim Zugriff auf den Browser oder eine Anwendung anzugeben.
- **Nicht nach meinem Master-Passwort fragen** - Sie werden beim Zugriff auf den Computer, einen Browser oder eine App nicht aufgefordert, Ihr Master-Passwort einzugeben.
- **Die Geldbörse automatisch sperren, wenn ich meinen PC verlasse** - Sie werden aufgefordert, Ihr Master-Passwort anzugeben, wenn Sie nach 15 Minuten an Ihren Computer zurückkehren.

**Wichtig**
Merken Sie sich Ihr Master-Passwort gut oder schreiben Sie es auf und verwahren es an einem sicheren Ort. Wenn Sie Ihr Passwort vergessen haben, müssen Sie das Programm neu installieren oder den Kundendienst von Bitdefender kontaktieren.

## Machen Sie es sich noch einfacher

So können Sie die Browser oder die Anwendungen auswählen, in die der Passwortmanager integriert werden soll:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **GELDBÖRSE**.
4. Wechseln Sie zum Reiter **PLUG-INS**.

   Wählen Sie eine Anwendung für die Nutzung des Passwortmanagers aus und machen Sie es sich noch einfacher:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Safepay

# Konfigurieren des automatischen Einfügens

Die Funktion für das automatische Einfügen erleichtert Ihnen den Zugriff auf Ihre Lieblingsseiten und das Anmelden bei Ihren Online-Konten. Ihre Anmeldedaten und persönlichen Daten werden bei der ersten Eingabe in Ihrem Web-Browser automatisch in der Geldbörse sicher gespeichert.

So können Sie die Einstellungen für das **automatische Einfügen** konfigurieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **GELDBÖRSE**.
4. Wechseln Sie zum Reiter **EINSTELLUNGEN AUTOM. EINFÜGEN**.
5. Entscheiden Sie sich für eine der folgenden Optionen:
   - **Legen Sie fest, wie die digitale Geldbörse Ihre Anmeldedaten absichern soll**:
     - **Anmeldedaten automatisch in der digitalen Geldbörse speichern** - Anmeldedaten und andere persönlich identifizierbare Daten wie Personendaten oder Kreditkarteninformationen werden in der Geldbörse automatisch gespeichert und aktualisiert.
     - **Immer fragen** - Sie werden jedes Mal gefragt, ob Ihre Anmeldedaten zur Geldbörse hinzugefügt werden sollen.
     - **Nicht speichern, ich möchte die Informationen manuell aktualisieren** - Die Anmeldedaten können nur von Hand zur Geldbörse hinzugefügt werden.
   - **Anmeldedaten automatisch einfügen**:
     - **Anmeldedaten immer automatisch einfügen** - Die Anmeldedaten werden automatisch im Browser eingefügt.
   - **Formulare automatisch ausfüllen**:
     - **Auf Formularseiten meine Ausfülloptionen anzeigen** - Ein Pop-up-Fenster mit Ihren Ausfülloptionen wird angezeigt, sobald Bitdefender erkennt, dass Sie eine Online-Zahlung vornehmen oder sich anmelden wollen.

## Passwortmanager-Daten über Ihren Browser verwalten

Sie können den Passwortmanager direkt über Ihren Browser verwalten, um jederzeit auf alle wichtigen Daten zugreifen zu können. Das Bitdefender-Geldbörse-Add-on wird von den folgenden Browsern unterstützt: Google Chrome, Internet Explorer und Mozilla Firefox. Darüber hinaus ist es auch in Safepay integriert

Um auf die Bitdefender-Geldbörse-Erweiterung zugreifen zu können, öffnen Sie Ihren Web-Browser, stimmen Sie der Installation des Add-ons zu und klicken Sie in der Symbolleiste auf das -Symbol.

Die Bitdefender-Geldbörse-Erweiterung bietet die folgenden Optionen:

- Geldbörse öffnen - Öffnet die Geldbörse.
- Geldbörse sperren - Sperrt die Geldbörse.
- Webseiten - Öffnet ein Untermenü mit allen in der Geldbörse gespeicherten Website-Anmeldedaten. Klicken Sie auf **Webseite hinzufügen**, um neue Websites zu der Liste hinzuzufügen.
- Formulare ausfüllen - Öffnet ein Untermenü mit den Informationen, die Sie für eine bestimmte Kategorie hinzugefügt haben. Hier können Sie neue Daten zu Ihrer Geldbörse hinzufügen.
- Passwortgenerator - Mit dem Passwortgenerator können Sie Zufallspasswörter für bestehende und neue Benutzerkonten erstellen. Klicken Sie auf **Erweiterte Einstellungen anzeigen**, um die Passwortkomplexität selbst zu konfigurieren.
- Einstellungen - Öffnet das Fenster für die Passwortmanager-Einstellungen.
- Problem melden - Hier können Sie alle Probleme melden, die im Zusammenhang mit dem Bitdefender-Passwortmanager auftreten.

# 4.11. VPN

Die VPN-App kann über Ihr Bitdefender-Produkt installiert werden und kann jederzeit genutzt werden, um Ihre Verbindung zusätzlich abzusichern. Das VPN dient als Tunnel zwischen Ihrem Gerät und dem Netzwerk, mit dem Sie sich verbinden. Ihre Verbindung wird abgesichert, Ihren Daten werden professionell nach Bankenstandard verschlüsselt und Ihre IP-Adresse bleibt

jederzeit unsichtbar. Ihr Datenverkehr wird über spezielle Server weitergeleitet, was es nahezu unmöglich macht, Ihr Gerät neben den unzähligen anderen Geräten zu identifizieren, die ebenfalls unsere Dienste in Anspruch nehmen. Darüber hinaus können Sie mit Bitdefender VPN im Internet auch auf solche Inhalte zugreifen, die üblicherweise regionalen Zugangsbeschränkungen unterliegen.

### Beachten Sie

In manchen Ländern wird Internetzensur betrieben. Aus diesem Grund ist die Nutzung von VPNs hier gesetzlich verboten. Um rechtliche Konsequenzen zu vermeiden, wird Ihnen bei der ersten Nutzung der Bitdefender-VPN-App eine Warnmeldung angezeigt. Durch die weitere Nutzung der App bestätigen Sie, dass Sie sich aller einschlägigen Rechtsvorschriften in Ihrem Land sowie der möglichen Risiken, denen Sie sich aussetzen, bewusst sind.

## VPN installieren

Gehen Sie wie folgt vor, um die VPN-App über Ihre Bitdefender-Benutzeroberfläche zu installieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **VPN** auf **VPN aktivieren**.
4. Lesen Sie in dem Fenster, in dem die VPN-App beschrieben wird, die **Abonnementvereinbarung** und klicken Sie danach auf **Bitdefender VPN AKTIVIEREN**.

   Warten Sie einen Moment, bis die Dateien heruntergeladen und installiert wurden.
5. Klicken Sie auf **BITDEFENDER VPN ÖFFNEN**, um die Installation abzuschließen.

### Beachten Sie

Bitdefender VPN erfordert zur Installation mindestens .Net Framework 4.5.2. Falls dieses Paket auf Ihrem Computer noch nicht installiert ist, wird ein Benachrichtigungsfenster angezeigt. Klicken Sie **.Net Framework installieren**, um auf eine Seite weitergeleitet zu werden, über die Sie die neueste Version dieser Software herunterladen können.

## Öffnen des VPN

Es gibt verschiedene Möglichkeiten, das Bitdefender VPN-Hauptfenster zu öffnen:

- Über die Task-Leiste
  1. Klicken Sie nach einem Rechtsklick auf das -Symbol in der Taskleiste auf **Anzeigen**.
- Über die Bitdefender-Benutzeroberfläche:
  1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
  2. Klicken Sie auf die **VPN**-Schaltfläche.

## VPN-Benutzeroberfläche

In der VPN-Benutzeroberfläche wird der Status der App angezeigt, verbunden oder getrennt. Der Serverstandort wird für Anwender mit der kostenlosen Version von Bitdefender automatisch auf den geeignetsten Server festgelegt. Premium-Anwender können dagegen den Serverstandort selbst wählen. Weitere Informationen zu den VPN-Abonnementen finden Sie unter *„Abonnements“* (S. 287).

Klicken Sie auf das Statussymbol oben auf dem Bildschirm oder klicken Sie mit der rechten Maustaste auf das Taskleistensymbol, um eine Verbindung herzustellen oder zu trennen. Auf dem Taskleistensymbol ist ein grüner Haken zu sehen, wenn das VPN verbunden ist. Ein roter Haken zeigt an, dass die VPN-Verbindung getrennt wurde.

Solange eine Verbindung besteht, wird die vergangene Zeit sowie die Ihrem Gerät automatisch zugewiesene IP-Adresse unten in der Benutzeroberfläche angezeigt.

Öffnen Sie das **Menü** mit einem Klick auf das -Symbol oben links , um auf weitere Optionen zuzugreifen. Dabei haben Sie die folgenden Möglichkeiten:

- **Mein Konto** - Hier werden Einzelheiten zu Ihrem Bitdefender-Benutzerkonto und Ihrem VPN-Abonnement angezeigt. Klicken Sie auf **Konto wechseln**, wenn Sie sich mit einem anderen Konto anmelden möchten.
- **Einstellungen** – Hier können Sie das Produktverhalten individuell anpassen:

- Erhalten Sie Benachrichtigungen, wenn das VPN Verbindungen automatisch herstellt oder trennt
- die VPN-App beim Windows-Systemstart automatisch ausführen
- die VPN-App automatisch starten, wenn Ihr Gerät mit einem ungesicherten WLAN-Netzwerk verbunden wird

- **Upgrade zur Premium-Version** - Falls Sie die kostenlose Produktversion nutzen, können Sie hier auf die Premium-Version upgraden.
- **Support** - Sie werden auf die Support Center-Platform weitergeleitet, wo Sie einen hilfreichen Artikel zur Nutzung der Bitdefender VPN lesen können.
- **Über** - Hier finden Sie Informationen zur installierten Version.

## Abonnements

Mit Bitdefender VPN erhalten Sie ein kostenloses Datenvolumen von 200 MB pro Tag, um Ihre Verbindung bei Bedarf abzusichern. Sie werden automatisch mit dem besten Serverstandort verbunden.

Wenn Sie sich für ein Upgrade auf die Premium-Version entscheiden, entfällt das Datenlimit und Sie können durch die freie Wahl des Serverstandorts Inhaltsbeschränkungen überall auf der Welt umgehen.

Mit einem Klick auf **UNBEGRENZTER DATENVERKEHR** können Sie über die Benutzeroberfläche jederzeit ein Upgrade auf Bitdefender Premium VPN durchführen.

Ein Bitdefender Premium-VPN-Abonnement läuft unabhängig von dem Bitdefender Total Security 2018-Abonnement, d. h. Sie können es über den gesamten Verfügbarkeitszeitraum hinweg nutzen, unabhängig vom Status des Abonnements Ihrer Sicherheitslösung. Wenn Ihr Bitdefender Premium-VPN-Abonnement abläuft, Ihr Bitdefender Total Security 2018-Abonnement aber weiterhin aktiv ist, kehren Sie zum kostenlosen Angebot zurück.

Bitdefender VPN ist ein plattformübergreifendes Produkt, das in Bitdefender-Produkten für Windows, macOS, Android und iOS verfügbar ist. Nach einem Premium-Upgrade können Sie Ihr Abonnement in allen Produkten nutzen, vorausgesetzt, dass Sie sich mit dem gleichen Bitdefender-Benutzerkonto anmelden.

## 4.12. Sichere Online-Transaktionen mit Safepay

Immer mehr Menschen nutzen ihren Computer regelmäßig für ihre Einkäufe und Bankgeschäfte. Rechnungen bezahlen, Überweisungen tätigen und einkaufen war noch nie schneller und einfacher.

Bei diesen Transaktionen werden personenbezogene Daten, Konto- und Kreditkartennummern, Passwörter und andere vertrauliche Informationen über das Internet übermittelt. Und das sind genau die Daten, die Online-Kriminelle so gerne in die Finger kriegen würden. Hacker lassen nichts unversucht, an diese Daten zu gelangen. Sie können also bei der Absicherung Ihrer Online-Transaktionen gar nicht vorsichtig genug sein.

Bitdefender Safepay™ ist zuallererst ein gesicherter Browser, ein abgeschottetes System, das speziell entwickelt wurde, damit Online-Transaktionen wie Einkäufe und Bankgeschäfte sicher und privat bleiben.

Um optimalen Privatsphärenschutz zu gewährleisten, wurde der Bitdefender-Passwortmanager in Bitdefender Safepay™ integriert, um Ihre Anmeldedaten jederzeit beim Aufrufen von privaten Seiten zu schützen. Weitere Informationen finden Sie unter *„Passwortmanager-Schutz für Ihre Anmeldedaten“ (S. 154)*.

Bitdefender Safepay™ hat die folgenden Vorteile:

- Es blockiert den Zugriff auf Ihren Desktop sowie sämtliche Versuche, Bildschirmfotos zu machen.
- So werden Ihre Passwörter im Internet mit dem Passwortmanager geschützt.
- Es hat eine eingebaute virtuelle Tastatur, die es Hackern unmöglich macht, Ihre Tastenanschläge aufzuzeichnen.
- Es ist völlig unabhängig von Ihren anderen Browsern.
- Es enthält den Hotspot-Schutz für Situationen, in denen Ihr Computer mit einem ungesicherten Funknetzwerk verbunden ist.
- Es hat eine Lesezeichenfunktion, mit der Sie mühelos auf Ihre Lieblings-Banking/Shopping-Seiten zugreifen können.
- Es ist nicht nur auf Online-Banking und -Shopping beschränkt. Jede Webseite kann in Bitdefender Safepay™ geöffnet werden.

# Bitdefender Safepay™ verwenden

Standardmäßig erkennt Bitdefender, wenn Sie auf Ihrem Computer über einen Browser eine Online-Banking-Seite oder einen Online-Shop aufrufen und fordert Sie auf, diese Seite in Bitdefender Safepay™ zu öffnen.

Es gibt verschiedene Möglichkeiten, das Bitdefender Safepay™-Hauptfenster zu öffnen:

- Über die Bitdefender-Benutzeroberfläche:
  1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
  2. Klicken Sie auf die **Safepay**-Schaltfläche.
- In Windows:
  - In **Windows 7**:
    1. Klicken Sie auf **Start** und **Alle Programme**.
    2. Klicken Sie auf **Bitdefender**.
    3. Klicken Sie auf **Bitdefender Safepay™**.
  - In **Windows 8 und Windows 8.1**:

    Finden Sie Bitdefender Safepay™ auf der Windows-Startseite (z.B. durch die Eingabe von "Bitdefender Safepay™" auf der Startseite) und rechtsklicken Sie auf das Symbol.
  - In **Windows 10**:

    Geben Sie "Bitdefender Safepay™" in das Suchfeld in der Taskleiste ein und klicken Sie auf das entsprechende Symbol.

### Beachten Sie

Falls das Adobe Flash Player Plugin nicht installiert oder nicht mehr aktuell ist, wird eine Bitdefender-Meldung angezeigt. Klicken Sie auf die entsprechende Schaltfläche, um fortzufahren.
Nach Abschluss des Installationsvorgangs müssen Sie den Bitdefender Safepay™-Browser erneut öffnen, um mit Ihrer Arbeit fortzufahren.

Wer schon einmal einen Internet-Browser benutzt hat, wird mit Bitdefender Safepay™ keinerlei Probleme haben - es sieht aus wie ein Browser und verhält sich auch so:

- Sie können URLs in die Adressleiste eingeben, um auf die entsprechende Seite zu gelangen.
- Sie können im Fenster von Bitdefender Safepay™ mehrere Reiter öffnen, indem Sie auf + klicken.
- Sie können über die Schaltflächen rückwärts und vorwärts durch bereits besuchte Seiten blättern und Seiten neu laden.
- die Bitdefender Safepay™-Einstellungen aufrufen, indem Sie auf klicken und **Einstellungen** auswählen.
- schützen Sie Ihre Passwörter mit dem Passwortmanager durch einen Klick auf .
- Sie können Ihre Lesezeichen mit einem Klick auf neben der Adressleiste verwalten.
- Sie können eine virtuelle Tastatur über die Schaltfläche öffnen.
- die Größe des Browser-Fensters durch gleichzeitiges Drücken von **Strg** und den **+/-**-Tasten im numerischen Tastenblock anpassen.
- Informationen über Ihr Bitdefender-Produkt aufrufen, indem Sie auf auf **Info über** auswählen.
- wichtige Informationen ausdrucken mit einem Klick auf .

### Beachten Sie

Drücken Sie **Alt+Tab** oder klicken Sie auf die **Minimieren**-Schaltfläche, um zwischen Bitdefender Safepay™ und dem Windows-Desktop zu wechseln.

## Einstellungen verändern

Klicken Sie auf und danach auf **Einstellungen**, um Bitdefender Safepay™ zu konfigurieren:

- In den **Allgemeinen Einstellungen** können Sie folgende Einstellungen vornehmen:

  **Verhalten von Bitdefender Safepay™**

  Hier können Sie einstellen, was passiert, wenn Sie die Seite eines Online-Shops oder eine Internet-Banking-Seite in einem normalen Browser aufrufen:
  - Websites automatisch in Safepay öffnen.
  - Verwendung von Safepay empfehlen.

- Verwendung von Safepay nicht empfehlen.

**Domain-Liste**

Hier können Sie einstellen, wie Bitdefender Safepay™ sich verhalten soll, wenn Sie Webseiten bestimmter Domains in Ihrem Standardbrowser aufrufen. Fügen Sie dazu einzelne Domains der Liste hinzu, und wählen Sie für jede eines der folgenden Verhalten:

- Automatisch in Bitdefender Safepay™ öffnen.
- Bitdefender soll Sie jedes Mal fragen, wie Sie vorgehen möchten.
- Bitdefender Safepay™ beim Aufruf von Seiten dieser Domain in einem Standardbrowser nie benutzen.

**Blockieren von Pop-ups**

Pop-ups können Sie mit einem Klick auf den entsprechenden Schalter blockieren.

Sie können auch eine Liste mit Websites anlegen, die Pop-ups anzeigen dürfen. Diese Liste sollte nur Websites enthalten, denen Sie uneingeschränkt vertrauen.

Um eine Website zu der Liste hinzuzufügen, geben Sie die Adresse in das entsprechende Feld ein und klicken Sie dann auf **Domain hinzufügen**.

Um eine Website aus der Liste zu löschen, klicken Sie auf das X für den jeweiligen Eintrag.

- In den **Erweiterten Einstellungen** stehen die folgenden Optionen zur Auswahl:

**Plug-ins verwalten**

Sie können selbst entscheiden, welche Plug-ins Sie in Bitdefender Safepay™ aktivieren oder deaktivieren möchten.

**Zertifikate verwalten**

Sie können Zertifikate von Ihrem System in einen Zertifikatspeicher importieren.

Wählen Sie **Zertifikate importieren** und folgen Sie den Anweisungen des Assistenten, um die Zertifikate in Bitdefender Safepay™. zu verwenden.

**Virtuelle Tastatur bei Passwortfeldern automatisch starten**

Die virtuelle Tastatur wird automatisch angezeigt, wenn ein Passwortfeld angewählt wird.

Über den entsprechenden Schalter können Sie die Funktion aktivieren oder deaktivieren.

**Vor dem Drucken Bestätigung anfordern**
Aktivieren Sie diese Option, wenn Sie eine Bestätigung geben möchten, bevor der Druckvorgang startet.

## Lesezeichen verwalten

Wenn Sie die automatische Erkennung einiger oder aller Websites deaktiviert haben oder Bitdefender einfach bestimmte Websites nicht korrekt erkennt, können Sie in Bitdefender Safepay™ Lesezeichen anlegen und so in Zukunft häufig besuchte Seiten schneller aufrufen.

So fügen Sie eine URL zu den Lesezeichen von Bitdefender Safepay™ hinzu:

1. Klicken Sie auf das -Symbol neben der Adressleiste, um die Lesezeichenliste zu öffnen.

   **Beachten Sie**
   Die Lesezeichenliste wird standardmäßig geöffnet, wenn Sie Bitdefender Safepay™ starten.

2. Klicken Sie auf das **+** um ein neues Lesezeichen hinzuzufügen.
3. Geben Sie die URL und den Namen für das Lesezeichen ein, und klicken Sie anschließend auf **Erstellen**. Aktivieren Sie die Option **Automatisch in Safepay öffnen**, wenn die in den Lesezeichen gespeicherte Seite bei jedem Besuch mit Bitdefender Safepay™ geöffnet werden soll. Die URL wird auch in der Domain-Liste auf der Seite Einstellungen hinzugefügt.

# 4.13. Datenschutz

## Endgültiges Löschen von Dateien

Wenn Sie eine Datei löschen, kann auf diese nicht mehr auf normalem Wege zugegriffen werden. Die Datei ist jedoch physisch solange weiterhin auf der Festplatte vorhanden, bis sie durch eine neue Datei überschrieben wird.

Der Bitdefender-Dateischredder hilft Ihnen, Daten endgültig zu löschen, indem er sie physisch von der Festplatte entfernt.

Wenn Sie das Windows-Kontextmenü nutzen möchten, um Dateien oder Ordner auf Ihrem Computer schnell und einfach zu schreddern, gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner, den Sie unwiderruflich löschen möchten.
2. Wählen Sie dann im Kontextmenü **Bitdefender** > **Dateischredder**.
3. Ein Bestätigungsfenster wird angezeigt. Klicken Sie auf **JA, LÖSCHENa**, um den Assistenten für den Dateischredder zu starten. Bitte warten Sie, bis Bitdefender das Schreddern der Dateien abgeschlossen hat.
4. Die Ergebnisse werden angezeigt. Klicken Sie auf **BEENDEN** um den Assistenten zu schließen.

Alternativ können Sie Dateien auch von innerhalb der Bitdefender-Oberfläche schreddern. Das geht so:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **DATENSCHUTZ** auf **Dateischredder**.
4. Befolgen Sie die Anweisungen des Dateischredderassistenten:
   a. Klicken Sie auf die Schaltfläche **ORDNER HINZUFÜGEN**, um die Dateien oder Ordner hinzuzufügen, die Sie dauerhaft löschen möchten.

      Alternativ können Sie diese Dateien oder Ordner mit der Maus auf dieses Fenster ziehen.

   b. Klicken Sie auf **DAUERHAFT LÖSCHEN** und bestätigen Sie, dass Sie mit dem Vorgang fortfahren möchten.

      Bitte warten Sie, bis Bitdefender das Schreddern der Dateien abgeschlossen hat.

   c. **Ergebnisübersicht**

      Die Ergebnisse werden angezeigt. Klicken Sie auf **BEENDEN** um den Assistenten zu schließen.

## 4.14. Elternberater

Mit dem Elternberater können Sie den Zugriff auf das Internet und bestimmte Anwendungen auf allen Geräten steuern, auf denen die Funktion installiert wird. Nach der Konfiguration des Elternberaters können Sie jederzeit nachvollziehen, wie Ihr Kind diese Geräte nutzt und wo es sich den vergangenen 24 Stunden aufgehalten hat. Darüber hinaus erstellt die App Statistiken über die Aktivitäten und Interessen des Kindes, um Sie noch besser auf dem Laufenden zu halten.

Sie benötigen nur einen Computer mit Internetzugang und einen Webbrowser.

Mit dem Elternberater können folgende Inhalte blockiert werden:

- Unangemessene Webseiten.
- Anwendungen wie Spiele, Chat, Filesharing-Programme oder Andere.
- bestimmte Kontakte, die keinen Telefonkontakt mit Ihrem Kind herstellen sollen.

Über Bitdefender-Konto können Sie von jedem beliebigen Computer oder Mobilgerät mit Internetzugang aus die Online-Aktivitäten Ihrer Kinder überwachen und die Einstellungen des Elternberaters anpassen.

### 4.14.1. Aufrufen des Elternberaters - MEINE KINDER

Rufen Sie den Bereich Elternberater auf, um das Fenster **MEINE KINDER** anzuzeigen. Hier können Sie alle Profile anzeigen und bearbeiten, die Sie für Ihre Kinder angelegt haben. Die Profile werden als Profilkarten angezeigt, über die Sie sie bequem verwalten und Ihren Status jederzeit einsehen können.

Nach Anlage eines Profils können Sie individuelle Einstellungen vornehmen, um den Zugriff Ihrer Kinder auf das Internet oder bestimmte Anwendungen zu überwachen und zu steuern.

Sie können über Bitdefender Central von jedem Computer oder Mobilgerät mit Internetzugang aus die Einstellungen des Elternberaters verändern.

Rufen Sie Ihr Bitdefender-Konto auf:

- Von einem beliebigen Gerät mit Internetzugang aus:
  1. Rufen Sie Bitdefender Central auf.

2. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Bitdefender-Konto an.
3. Wählen Sie die Funktion **Elternberater** aus.
4. Das Fenster **MEINE KINDER** wird angezeigt. Hier können Sie die Elternberater-Profile für jedes Gerät verwalten und konfigurieren.

- Über Ihre Bitdefender-Benutzeroberfläche:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **ELTERNBERATER** auf **Konfigurieren**.

   Sie werden auf die Bitdefender-Konto Website weitergeleitet. Stellen Sie sicher, dass Sie sich mit Ihren Anmeldedaten angemeldet haben.
4. Wählen Sie die Funktion **Elternberater** aus.
5. Das Fenster **MEINE KINDER** wird angezeigt. Hier können Sie die Elternberater-Profile für jedes Gerät verwalten und konfigurieren.

**Beachten Sie**
Stellen Sie sicher, dass Sie auf dem Computer eingeloggt sind, auf dem sich das Administrator-Benutzerkonto befindet. Nur Benutzer mit administrativen Rechten (Systemadministratoren) können auf den Elternberater zugreifen und ihn konfigurieren.

## 4.14.2. Profile Ihrer Kinder anlegen

Um die Aktivitäten Ihres Kindes überwachen zu können, müssen Sie zunächst ein Profil konfigurieren und die Anwendung für den Bitdefender-Elternberater auf dem von ihm verwendeten Gerät installieren.

So können Sie das Profil Ihres Kindes zum Elternberater hinzufügen:

1. Öffnen Sie den Bereich Elternberater in Bitdefender Central.
2. Klicken Sie rechts im Fenster **MEINE KINDER** auf **PROFIL HINZUFÜGEN**.
3. Geben Sie weitere Informationen wie Name und Geburtsdatum in die entsprechenden Felder ein. Um ein Profil-Foto hinzuzufügen, klicken Sie auf den Link **Datei auswählen**. Klicken Sie auf **NÄCHSTER SCHRITT**.

Basierend auf Erkenntnissen zur Kindesentwicklung werden bei der Eingabe des Geburtsdatums des Kindes automatisch altersgerechte Einstellungen für die Internet-Suche voreingestellt.

4. Falls Bitdefender Total Security 2018 bereits auf dem Gerät Ihres Kindes installiert ist, wählen Sie dieses Gerät aus der entsprechenden Liste aus und dann das Konto, das Sie überwachen möchten. Klicken Sie auf **SPEICHERN**.

   Falls Ihr Kind ein Android- oder iOS-Gerät verwendet und der Bitdefender-Elternberater nicht installiert ist, klicken Sie auf **GERÄT HINZUFÜGEN**. Falls Ihr Kind ein Mac-Gerät verwendet und die App für Bitdefender Antivirus for Mac nicht installiert ist, klicken Sie auf die gleiche Schaltfläche. Wählen Sie das Betriebssystem aus, für das Sie die App installieren möchten und klicken Sie auf **NÄCHSTER SCHRITT**, um fortzufahren.

5. Geben Sie die E-Mail-Adresse ein, an die wir den Download-Link für die Installation der Bitdefender-App senden sollen und klicken Sie anschließend auf **INSTALLATIONSLINK SENDEN**.

**Wichtig**

Auf Windows-basierten Geräten muss das Bitdefender Total Security 2018-Produkt, das in Ihrem Abonnement enthalten ist, heruntergeladen und installiert werden.

Auf macOS-Geräten muss das Bitdefender-Antivirus-for-Mac-Produkt heruntergeladen und installiert werden.

Auf Android- und iOS-Geräten muss die Anwendung für den Bitdefender-Elternberater heruntergeladen und installiert werden.

## Zuordnung mehrerer Geräte zum gleichen Profil

Sie können einem Profil gleich mehrere Geräte zuordnen und so auf allen Geräten die gleichen Einschränkungen vornehmen. Gehen Sie dazu folgendermaßen vor:

1. Rufen Sie Bitdefender Central auf.
2. Wählen Sie die Funktion Elternberater aus.
3. Klicken Sie auf der gewünschten Profilkarte auf das ⋮-Symbol and anschließend auf **Geräte**.

4. Wählen Sie aus der Liste die verfügbaren Geräte, denen Sie das Profil zuweisen möchten.

   Falls Ihr Kind ein Android- oder iOS-Gerät verwendet und der Bitdefender-Elternberater nicht installiert ist, klicken Sie auf **GERÄT HINZUFÜGEN**. Falls Ihr Kind ein Mac-Gerät verwendet und die App für Bitdefender Antivirus for Mac nicht installiert ist, klicken Sie auf die gleiche Schaltfläche. Wählen Sie das Betriebssystem aus, für das Sie die App installieren möchten und klicken Sie auf **NÄCHSTER SCHRITT**, um fortzufahren.

   Geben Sie die E-Mail-Adresse ein, an die wir den Download-Link für die Installation der Bitdefender-App senden sollen und klicken Sie anschließend auf **INSTALLATIONSLINK SENDEN**.

5. Nach Abschluss des Installationsvorgangs auf dem neuen Gerät können Sie das entsprechende Gerät aus der Liste auswählen und das Profil zuweisen.

6. Klicken Sie auf **SPEICHERN**.

## Verknüpfen des Elternberaters mit Bitdefender Central

Um die Online-Aktivitäten Ihres Kindes auf Android- und iOS-Geräten zu überwachen, müssen Sie das Gerät Ihres Kindes mit Ihrem Bitdefender-Konto verknüpfen, indem Sie sich über die App bei Ihrem Konto anmelden.

So können Sie ein Gerät mit Ihrem Bitdefender-Konto verknüpfen:

- Unter **Android**:

  1. Klicken Sie auf die Schaltfläche, die in der von unserem Server versandten E-Mail angezeigt wird. Sie werden zum Google Play Store weitergeleitet.

     Falls Sie über Ihr Bitdefender-Konto nicht den Versand eines Download-Links an die E-Mail-Adresse Ihres Kindes angefragt haben, können Sie die Bitdefender-Elternberater-App in Google Play selbst aufrufen.

  2. Tippen Sie im Fenster für den Bitdefender-Elternberater auf **INSTALLIEREN**. Tippen Sie auf **AKZEPTIEREN**, um den angefragten Berechtigungen zuzustimmen. Bitdefender benötigt diese Berechtigungen, um Sie über die Aktivitäten Ihres Kindes auf dem

Laufenden zu halten. Die App kann ohne diese Berechtigungen nicht installiert werden.

3. Öffnen Sie Sie Elternberater-App.
4. Lesen Sie den **Abonnementvereinbarung** und tippen Sie auf **FORTFAHREN**.
5. Melden Sie sich bei Ihrem bestehenden Bitdefender-Benutzerkonto an oder melden Sie sich mit einem Google-Benutzerkonto an.

   Falls Sie noch kein Bitdefender-Benutzerkonto haben, können Sie über die entsprechende Option ein neues Konto anlegen.
6. Tippen Sie auf **EINSTELLUNGEN AUFRUFEN**, um die Einstellungen aufzurufen, über die Sie die Eingabehilfe-Option für die App aktivieren können. Befolgen Sie die Anleitung auf dem Bildschirm, um die App ordnungsgemäß einzurichten.
7. Tippen Sie auf **EINSTELLUNGEN AUFRUFEN**, um die Einstellungen aufzurufen, über die Sie die Option Zugriff auf die Nutzungsdaten für die App aktivieren können. Befolgen Sie die Anleitung auf dem Bildschirm, um die App ordnungsgemäß einzurichten.
8. Tippen Sie auf **EINSTELLUNGEN AUFRUFEN**, um die Einstellungen aufzurufen, über die Sie die Option zur Aktivierung der Geräteadministratorrechte für die App aktivieren können. Befolgen Sie die Anleitung auf dem Bildschirm, um die App ordnungsgemäß einzurichten.

   So verhindern Sie, dass Ihr Kind die Elternberater-Anwendung deinstalliert.
9. Tippen Sie auf **FERTIG**, um den Installationsvorgang abzuschließen.

   **Beachten Sie**
   Ab Android 4.4 muss Bitdefender für die Überwachung der SMS-Nachrichten Ihrer Kinder zunächst die Einstellungen der integrierten Android-Messages-App anpassen. Wir empfehlen, dass Sie im Pop-up-Fenster, das nach dem Antippen von **FERTIG** in der App angezeigt wird, **Ja** auswählen.

- Unter **iOS**:

1. Klicken Sie auf Schaltfläche, die in der von unserem Server versandten E-Mail angezeigt wird, und installieren Sie die App.

2. Öffnen Sie Sie Elternberater-App.
3. Ein Assistent mit näheren Informationen zu den Produktfunktionen wird angezeigt. Klicken Sie zum Fortfahren auf **Weiter**.
4. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Bitdefender-Konto an.
5. Erlauben Sie den Zugriff auf den Standort des Gerätes, damit Bitdefender es orten kann.
6. Erlauben Sie der App den Versand von Benachrichtigungen.
7. Weisen Sie das Gerät dem Profil Ihres Kindes zu.

## Überwachen der Aktivitäten Ihrer Kinder

Mit Bitdefender können Sie jederzeit nachvollziehen, was Ihre Kinder im Internet machen.

Sie können aufzeichnen, welche Websites sie besuchen, welche Anwendungen sie gestartet haben und welche Aktivitäten vom Elternberater blockiert wurden.

Je nachdem welche Einstellungen Sie vorgenommen haben, enthalten die Berichte detaillierte Informationen zu jedem Ereignis, so zum Beispiel:

- Der Status des Vorgangs.
- Schweregrad der Benachrichtigung.
- Der Name des Geräts.
- Zeitpunkt, zu dem der Vorgang passiert ist.

So können Sie den Internet-Datenverkehr, die aufgerufenen Anwendungen und die Facebook-Aktivitäten Ihrer Kinder überwachen:

1. Öffnen Sie den Bereich Elternberater in Bitdefender Central.
2. Wählen Sie die gewünschte Gerätekarte aus.

   Im Fenster **Aktivität** können Sie die für Sie interessanten Informationen abrufen. Alternativ können Sie auf den Link **Heutige Aktivität anzeigen** auf der Karte des überwachten Geräts klicken. Damit werden Sie zum Fenster **Aktivität** weitergeleitet.

## Konfigurieren der allgemeinen Einstellungen

Standardmäßig werden bei aktiviertem Elternberater die Aktivitäten Ihrer Kinder aufgezeichnet.

So erhalten Sie E-Mail-Benachrichtigungen:

1. Öffnen Sie den Bereich Elternberater in Bitdefender Central.
2. Klicken Sie oben rechts auf den Reiter **Einstellungen**.
3. Aktivieren Sie die entsprechende Option, um Aktivitätsberichte zu erhalten.
4. Geben Sie die E-Mail-Adresse ein, an die die E-Mail-Benachrichtigungen gesendet werden sollen.
5. Sie erhalten E-Mail-Benachrichtigungen über:
   - Blockierte Websites
   - Blockierte Anwendungen
   - Unsichere Zonen
   - Eingegangener Anrufe oder eingegangene SMS von einer blockierten Telefonnummer
   - Entfernung der Facebook-Elternberater-App
6. Klicken Sie auf **SPEICHERN**.

## Bearbeiten eines Profils

So bearbeiten Sie ein bestehendes Profil:

1. Rufen Sie Bitdefender Central auf.
2. Rufen Sie den Bereich **Elternberater** auf.
3. Klicken Sie auf das ⋮ -Symbol auf der gewünschten Profilkarte und wählen Sie **Bearbeiten** aus.
4. Passen Sie die Einstellungen wie gewünscht an und klicken Sie dann auf **SPEICHERN**.

## Entfernen eines Profils

So entfernen Sie ein bestehendes Profil:

1. Rufen Sie Bitdefender Central auf.

2. Rufen Sie den Bereich **Elternberater** auf.
3. Klicken Sie auf das ⋮ -Symbol auf der gewünschten Profilkarte und wählen Sie **Entfernen** aus.
4. Bestätigen Sie Ihre Auswahl.

### 4.14.3. Konfigurieren der Elternberater-Profile

Um die Aktivitäten Ihres Kindes überwachen zu können, müssen Sie dem Gerät, auf dem der Bitdefender-Elternberater installiert wurde, zunächst ein Profil zuordnen.

Nachdem Sie ein Profil für Ihr Kind hinzugefügt haben, können Sie die Einstellungen individuell anpassen, um den Zugriff auf das Internet und bestimmte Anwendungen zu überwachen und zu steuern.

Um ein Profil zu konfigurieren, müssen Sie zunächst die entsprechende Profilkarte im Fenster **MEINE KINDER** auswählen.

Klicken Sie auf einen Reiter, um die entsprechende Elternberater-Funktion für das Gerät zu konfigurieren:

- Aktivität - Zeigt alle Aktivitäten, Interessen, Aufenthaltsorte und Interaktionen mit Freunden für den aktuellen Tag.
- Anwendungen - Erlaubt Ihnen, den Zugriff auf bestimmte Anwendungen wie Spiele, Chat-Dienste oder Filme zu blockieren.
- Websites - Hier können Sie das Surf-Verhalten filtern.
- Telefonkontakte - Hier können Sie festlegen, welche Telefonkontakte Ihr Kind anrufen dürfen.
- Standort des Kindes - Hier können Sie sichere und unsichere Zonen für Ihr Kind festlegen.
- Sozial - Hier können Sie den Zugang zu sozialen Netzwerken blockieren.
- Zeitplan - Hiermit können Sie den Zugang zu Geräten sperren, die Sie im Profil Ihres Kindes hinterlegt haben.

#### Aktivität

Im Aktivitätsfenster erhalten Sie detaillierte Informationen zu den Aktivitäten Ihrer Kinder in den letzten 24 Stunden, zuhause und unterwegs. Die Aktivitäten

der vergangenen Tage können Sie anzeigen, indem Sie links oben auf das Kalendersymbol klicken.

Je nach Aktivität umfassen die in diesem Fenster angezeigten Informationen zum Beispiel:

- **Aufenthaltsorte** - Hier können Sie die Aufenthaltsorte Ihres Kindes am aktuellen Tag nachvollziehen.
- **Interessen** - Hier können Sie Informationen zu den Website-Kategorien einsehen, die Ihr Kind aufgerufen hat. Klicken Sie auf **Unangemessene Inhalte prüfen**, um den Zugang zu verschiedenen Interessengebieten zu erlauben oder zu verweigern.
- **Soziale Interaktionen** - Hier können Sie nachvollziehen, mit welchen Kontakten Ihr Kind kommuniziert hat. Klicken Sie auf **Kontakte verwalten**, um festzulegen, mit welchen Kontakten Ihr Kind Kontakt treten darf oder nicht.
- **Anwendungen** - Hier finden Sie die Apps, die Ihr Kind verwendet hat. Klicken Sie auf **App-Einschränkungen überprüfen**, um den Zugriff auf bestimmte Anwendungen zuzulassen oder zu blockieren.
- **Ganztägige Aktivität** - Hier können Sie nachverfolgen, wie viel Zeit Ihr Kind mit dem ihm zugewiesenen Geräten im Internet verbracht hat und wo es sich aufgehalten hat. Die gesammelten Informationen beziehen sich dabei auf den jeweils aktuellen Tag.

## Anwendungen

Über das Anwendungsfenster können Sie verhindern, dass bestimmte Anwendungen ausgeführt werden. So können Sie jede beliebige Anwendung sperren – neben Spiel-, Medien- und Chatprogrammen auch andere Arten von Software.

Die Funktion kann über den entsprechenden Schalter aktiviert oder deaktiviert werden.

Konfiguration der Programmkontrolle für ein bestimmtes Benutzerkonto:

1. Eine Liste mit Karten wird angezeigt. Die Karten zeigen die von Ihrem Kind verwendeten Apps.
2. Wählen Sie die Karte mit der App aus, die Ihr Kind nicht mehr verwenden soll.

Ein Häkchen-Symbol zeigt an, dass Ihr Kind die App nicht mehr aufrufen kann.

## Webseiten

Über das Websites-Fenster können Sie Websites mit unangemessenen Inhalten blockieren. Auf diese Weise können Sie Websites blockieren, auf denen Videos, Spiele, Medieninhalte oder Chat-Programme bereitgestellt werden.

Die Funktion kann über den entsprechenden Schalter aktiviert oder deaktiviert werden.

Die Interessenliste und die Auswahl der aktivierten Kategorien richtet sich standardmäßig nach dem Alter, das Sie für Ihr Kind angegeben haben. Klicken Sie auf eine Kategorie, um den Zugriff darauf zu erlauben oder zu verweigern.

Ein Häkchen-Symbol zeigt an, dass Ihr Kind keine Inhalte aus der jeweiligen Kategorie abrufen kann.

### Zulassen oder Blockieren einer Website

Um den Zugriff auf bestimmte Websites zu erlauben oder einzuschränken, müssen Sie sie wie folgt zur Ausschlussliste hinzufügen:

1. Klicken Sie auf die Schaltfläche **VERWALTEN**.
2. Geben Sie die Adresse der Website, zu der Sie den Zugriff erlauben oder blockieren möchten, in das entsprechende Feld ein.
3. Wählen Sie **Zulassen** oder **Blockieren** aus.
4. Klicken Sie auf **Beenden**, um die Änderungen zu speichern.

**Beachten Sie**
Einschränkungen für den Website-Zugriff können nur für Windows-, Android- und macOS-Geräte festgelegt werden, die dem Profil Ihres Kindes hinzugefügt wurden.

## Telefonkontakte

Im Fenster Telefonkontakte können Sie festlegen, welche Freunde aus der Kontaktliste Ihr Kind anrufen darf und welche nicht.

Wenn Sie die Telefonnummer eines Kontakts sperren möchten, müssen Sie zunächst das Android-Gerät Ihres Kindes zu seinem Profil hinzufügen. Das geht so:

1. Wechseln Sie in Bitdefender Central zum Reiter **Elternberater**.
2. Klicken Sie auf der gewünschten Karte auf **Elternberater auf einem Gerät installieren**.
3. Klicken Sie im angezeigten Fenster auf **GERÄT HINZUFÜGEN**.
4. Die Option **Bitdefender-Elternberater für Android** ist standardmäßig ausgewählt. Klicken Sie auf **NÄCHSTER SCHRITT**.
5. Wählen Sie das Profil des Kindes aus, für das Sie die Beschränkungen festlegen möchten.
6. Klicken Sie auf den Reiter **Telefonkontakte**.

   Eine Liste mit Karten wird angezeigt. Die Karten zeigen die Kontakte auf dem Android-Smartphone Ihres Kindes.
7. Wählen Sie die Karte mit der Telefonnummer aus, die Sie blockieren möchten.

   Ein Häkchen-Symbol zeigt an, dass Ihr Kind von der ausgewählten Nummer nicht mehr angerufen werden kann.

Aktivieren Sie den Schalter **Unbekannte Nummern blockieren**, um unbekannte Telefonnummern zu blockieren.

> **Beachten Sie**
> Anrufeinschränkungen können nur für Android-Geräte festgelegt werden, die dem Profil Ihres Kindes hinzugefügt wurden.

## Aufenthaltsort des Kindes

Hier können Sie den aktuellen Gerätestandort in Google Maps anzeigen. Der Standort wird alle 5 Sekunden aktualisiert, eine Bewegung kann also nachverfolgt werden.

Die Genauigkeit der Ortung hängt davon ab, wie gut Bitdefender seinen Standort bestimmen kann:

- Wenn GPS im Gerät aktiviert ist, kann sein Standort bis auf ein paar Meter genau bestimmt werden, solange das Gerät in Reichweite der GPS-Satelliten (d. h. nicht in einem Gebäude) ist.

- Wenn sich das Gerät in einem Gebäude befindet, kann sein Standort auf mehrere zehn Meter genau bestimmt werden, solange WLAN aktiviert ist und Drahtlosnetzwerke in Reichweite des Geräts sind.
- Andernfalls wird der Standort allein über Daten aus dem Mobilfunknetzwerk bestimmt, wodurch die Genauigkeit auf einen Umkreis von ein paar hundert Metern sinkt.

## Konfigurieren von Standort & Rückmeldung

Um sicherzugehen, wo Ihr Kind sich aufhält, können Sie eine Liste mit sicheren und unsicheren Orten anlegen. Kommt Ihr Kind jetzt alleine einen im Voraus festgelegten Bereich an, wird es per Benachrichtigung in der Elternberater-App dazu aufgefordert, Sie über seine sichere Ankunft zu informieren. Tippt es danach auf **ICH BIN GUT ANGEKOMMEN**, werden Sie über eine Benachrichtigung in Ihrem Bitdefender-Benutzerkonto über die sichere Ankunft am Zielort informiert.

Falls Ihr Kind keine Bestätigung schickt, können Sie in seinem Profil in Ihrem Bitdefender-Benutzerkonto den Standortverlauf für den Tag einsehen.

So legen Sie einen Aufenthaltsort fest:

1. Im Fenster **Standort des Kindes** wird ein Rahmen angezeigt. Klicken Sie hier auf **Geräte**.
2. Klicken Sie auf **GERÄTE AUSWÄHLEN** und wählen Sie das zu konfigurierende Gerät aus.
3. Klicken Sie im Fenster **Zonen** auf die **ZONE HINZUFÜGEN**-Schaltfläche.
4. Wählen Sie aus, ob der Ort als **SICHER** oder **UNSICHER** gelten soll.
5. Geben Sie einen gültigen Namen für die Zone ein, die Ihre Kinder aufsuchen bzw. nicht aufsuchen dürfen.
6. Legen Sie über den **Radius**-Regler einen Überwachungsradius fest.
7. Klicken Sie auf **ZONE HINZUFÜGEN**, um Ihre Einstellungen zu speichern. Sie werden gefragt, ob Ihre Kinder alleine unterwegs sind oder nicht. Antworten Sie mit ja oder nein.

### Beachten Sie

Die Standortverfolgung kann zur Überwachung von Android- und iOS-Geräten verwendet werden, auf denen die Bitdefender-Elternberater-App installiert ist.

## Sozial

Mit dem Elternberater können Sie auch das Facebook-Konto Ihres Kindes überwachen und Berichte über die wichtigsten Aktivitäten dort erstellen.

Die Online-Aktivitäten werden geprüft, und eine Warnung wird ausgegeben, wenn sie eine Gefahr für die Privatsphäre Ihres Kindes darstellen sollten.

Überwacht werden die folgenden Elemente:

- Kontoinformationen
- Gefällt-mir-Angaben
- hochgeladene Bilder

Um den Facebook-Schutz für ein bestimmtes Benutzerkonto zu konfigurieren, geben Sie die E-Mail-Adresse des überwachten Benutzerkontos Ihres Kindes ein und klicken Sie danach auf **SENDEN**.

Informieren Sie Ihr Kind über Ihr Vorhaben und bitten Sie es, in der von uns erhaltenen E-Mail die Schaltfläche **KONTO SCHÜTZEN** anzuklicken.

Klicken Sie auf den Link **Auf Facebook ansehen**, um auf das überwachte Facebook-Konto zuzugreifen.

Um die Überwachung des Kontos zu beenden, klicken Sie oben auf die **KONTOVERKNÜPFUNG AUFHEBEN**-Schaltfläche.

Aktivieren Sie das entsprechende Kästchen, um per E-Mail informiert zu werden, wenn Ihr Kind die Elternberater-App von seinem Gerät entfernt.

## Zeitplan

Im Zeitplan-Fenster können Sie den Zugang Ihres Kindes zu den Geräten, die Sie im Profil des Kindes festgelegt haben, einschränken. Einschränkungen können jederzeit während der Unterrichtszeit und an Wochenenden, jedoch ausschließlich für Android- und Windows-Geräte festgelegt werden.

So richten Sie eine Zeitbegrenzung abends/nachts ein:

1. Markieren Sie im Bereich **ABENDS/NACHTS** die Kästchen **Schultag abends/nachts** und **Wochenende abends/nachts**.
2. Klicken Sie an den entsprechenden Einstellfeldern auf das ⊗-Symbol und stellen Sie dann mit den Pfeiltasten der Tastatur die Intervalle ein, während der der Zugang blockiert werden soll.

So richten Sie eine Zeitbegrenzung tagsüber ein:

1. Im Bereich**BEGRENZUNGEN TAGSÜBER** haben Sie folgende Optionen:
   - **KUMULATIV**
     a. Markieren Sie die Kästchen **Zeitbegrenzung Schultag** und **Zeitbegrenzung Wochenende**.
     b. Stellen Sie mithilfe der Schieber ein, für wie lange der Zugang erlaubt ist.
   - **KONKRET**
     a. Markieren Sie die Kästchen **Zeitbegrenzung Schultag** und **Zeitbegrenzung Wochenende**.
     b. Wählen Sie im Raster die Zeitintervalle, in denen der Zugang blockiert werden soll.

> **Beachten Sie**
> Die Einstellungen **KUMULATIV** und **KONKRET** funktionieren unabhängig voneinander.

## 4.15. Diebstahlschutz

Laptop-Diebstahl ist ein ernstzunehmendes Problem für Privatleute wie für Firmen. Schwerer noch als der Verlust der Hardware selbst wiegt dabei der Verlust der Daten, sowohl materiell wie emotional.

Und doch sichern nur Wenige ihre wichtigen persönlichen und geschäftlichen Daten gegen Diebstahl hinreichend ab.

Der Bitdefender-Diebstahlschutz gibt Ihnen im Falle eines Diebstahls die Möglichkeit, Ihren Laptop aus der Ferne zu orten und zu sperren und sogar sämtliche Daten zu löschen.

Der Diebstahlschutz funktioniert nur unter den folgenden Bedingungen:

- Die Befehle können nur über das Bitdefender-Benutzerkonto gesendet werden.
- Der Laptop muss mit dem Internet verbunden sein, um die Befehle zu empfangen.

Der Diebstahlschutz hat die folgenden Funktionen:

**Orten**

Hiermit können Sie den Standort Ihres Geräts in Google Maps anzeigen.

Die Genauigkeit der Ortung hängt davon ab, auf welche Weise Bitdefender den Standort bestimmt. Der Standort wird auf einige zehn Meter genau bestimmt, sofern WLAN auf Ihrem Laptop aktiviert ist und Funknetzwerke innerhalb seiner Reichweite sind.

Wenn der Computer mit einem verkabelten LAN verbunden ist und eine WLAN-basierte Ortung nicht möglich ist, wird der Standort über die IP-Adresse ermittelt, was deutlich ungenauer ist.

**Alarm**

Senden Sie eine Benachrichtigung an das Gerät.

Diese Funktion ist nur für Mobilgeräte verfügbar.

**Sperren**

Den Computer sperren und eine 4-stellige PIN zur Entsperrung festlegen. Wenn Sie den Befehl zum **Sperren** senden, führt der Computer einen Neustart durch, wonach Windows nur noch über die Eingabe der von Ihnen festgelegten PIN zugänglich ist.

Wenn Bitdefender Fotos von allen Personen aufnehmen soll, die auf Ihr Laptop zugreifen wollen, aktivieren Sie das entsprechende Kästchen. Die Fotos werden über die Frontkamera aufgenommen und werden gemeinsam mit dem Zeitstempel im Diebstahlschutz-Dashboard angezeigt. Es werden nur die zwei aktuellsten Fotos gespeichert.

Diese Funktion steht nur auf Laptops mit Frontkamera zur Verfügung.

**Löschen**

Entfernen Sie alle Daten von Ihrem System. Wenn Sie den Befehl zu **Löschung** senden, führt der Laptop einen Neustart durch und löscht sämtliche Daten auf allen Festplattenpartitionen.

**IP anzeigen**

Zeigt die letzte IP-Adresse für das ausgewählte Gerät an. Klicken Sie auf **IP ANZEIGEN**, um sie sichtbar zu machen.

Der Diebstahlschutz wird nach der Installation aktiviert und kann nur über Ihr Bitdefender-Konto von einem beliebigen mit dem Internet verbundenen Gerät aus genutzt werden.

## Verwendung der Diebstahlschutz-Funktionen

Es gibt verschiedene Möglichkeiten, die Diebstahlschutzfunktionen aufzurufen:

- Über das Bitdefender-Hauptfenster:
  1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
  2. Klicken Sie auf die **Diebstahlschutz**-Schaltfläche.
  3. Ein neues Bitdefender Central-Fenster wird geöffnet. Klicken Sie auf die entsprechende Gerätekarte und wählen Sie **Diebstahlschutz** aus.
- Von einem beliebigen Gerät mit Internetzugang aus:
  1. Rufen Sie über Ihren Web-Browser https://central.bitdefender.com auf.
  2. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Bitdefender-Konto an.
  3. Rufen Sie den Bereich **Meine Geräte** auf.
  4. Klicken Sie auf die entsprechende Gerätekarte und wählen Sie **Diebstahlschutz** aus.
  5. Wählen Sie die Funktion, die Sie verwenden möchten:

     **IP anzeigen** - Zeigt die letzte IP-Adresse Ihres Geräts an.
     **Orten** - zeigt den Standort Ihres Geräts auf Google Maps.
     **Benachrichtigung** - Schickt eine Benachrichtigung auf das Gerät.
     **Sperren** - den Laptop sperren und eine PIN zum Entsperren festlegen.
     **Löschen** - sämtliche Daten von Ihrem Laptop löschen.

     **Wichtig**
     Nach einer Löschung funktionieren die Diebstahlschutz-Funktionen nicht mehr.

# 4.16. USB Immunizer

Die Autostart-Funktion, die in jedem Windows-Betriebssystem angelegt ist, ist sehr praktisch, denn über sie kann der Computer direkt Dateien auf angeschlossenen Medien ausführen. So werden zum Beispiel eine Installation sofort gestartet, wenn die Installations-CD der Software eingelegt wird.

Leider können Bedrohungen diese Funktion missbrauchen, um sich automatisch von beschreibbaren Medien wie USB-Sticks und Speicherkarten aus auf Ihrem System einzunisten. In der letzten Zeit ist die Zahl der Angriffe über die Autostart-Funktion gewachsen.

Mit der USB-Immunisierung können Sie verhindern, dass mit NTFS, FAT32 oder FAT formatierte Flash-Speicher je wieder automatisch Bedrohungen ausführen. Wenn ein USB-Gerät einmal immunisiert wurde, kann es nicht mehr durch Bedrohungen dazu gebracht werden, eine bestimmte Anwendung auszuführen, sobald es mit einem Windows-Computer verbunden wird.

So können Sie USB-Geräte immunisieren:

1. Verbinden Sie das Flash-Laufwerk mit Ihrem Computer.
2. Suchen Sie das Gerät auf Ihrem Arbeitsplatz und klicken Sie mit der rechten Maustaste darauf.
3. Wählen Sie im Kontextmenü **Bitdefender** und anschließend **Dieses Laufwerk immunisieren**.

> **Beachten Sie**
> Wenn das Laufwerk bereits immunisiert wurde, wird anstatt der Immunisierungsoption folgende Meldung angezeigt: **Das USB-Gerät ist jetzt gegen Autostart-Bedrohungen geschützt.**

Sie können auch verhindern, dass Ihr Computer Bedrohungen von nicht immunisierten USB-Geräten startet, indem Sie die Autostart-Funktion deaktivieren. Weitere Informationen finden Sie unter *„Automatische Schwachstellensuche“* (S. 136).

# 5. SYSTEMOPTIMIERUNG

## 5.1. Extras

Bitdefender enthält einen Bereich mit Extras, der Ihnen hilft, die Unversehrtheit Ihres Systems zu bewahren. Die Wartungsprogramme sind wichtig für die Verbesserung der Reaktionszeit Ihres Systems und die effiziente Verwaltung des Festplattenspeichers.

Bitdefender bietet die folgenden PC-Tuning-Tools:

- Die Ein-Klick-Optimierung analysiert und verbessert Ihre Systemgeschwindigkeit, indem es mit nur einem Klick eine Vielzahl an Aufgaben ausführt.
- Die Systemstartoptimierung verhindert, dass beim Systemstart nicht benötigte Anwendungen geladen werden, um die Startzeit zu verkürzen.
- Disk Cleanup findet Dateien, die möglicherweise für Ihr Speicherplatzproblem verantwortlich sind, und gibt Ihnen die Möglichkeit, diese bei Bedarf zu löschen.

### 5.1.1. Optimierung der Systemgeschwindigkeit mit nur einem Klick

Probleme wie Festplattenausfälle, nicht mehr benötigte Registry-Dateien und Browser-Verläufe können Ihren Computer ausbremsen und äußerst lästig werden. All diese Probleme können mit nur einem Klick behoben werden.

Die Ein-Klick-Optimierung ermöglicht das Auffinden und die Entfernung von nicht mehr benötigten Dateien indem es eine Vielzahl von Bereinigungsaufgaben gleichzeitig ausführt.

So können Sie den Prozess für die Ein-Klick-Optimierung starten:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf die Schaltfläche **Ein-Klick-Optimierung**.
   a. **Analyse**

      Bitte warten Sie, bis Bitdefender die Suche nach Systemproblemen abgeschlossen hat.

- Disk Cleanup - findet nicht mehr benötigte Dateien und Ordner.
- Registry-Bereinigung - Findet ungültige oder verwaiste Referenzen in der Windows-Registry.
- Datenschutz-Bereinigung - Findet temporäre Internet-Dateien und Cookies sowie Browser-Cache und -Verlauf.

Die Anzahl der gefundenen Probleme wird angezeigt. Diese sollten mit einem Klick auf **Details anzeigen** überprüft werden, bevor Sie mit dem Bereinigungsprozess fortfahren. Klicken Sie zum Fortfahren auf **OPTIMIEREN**.

b. **Optimierung**

Bitte warten Sie, bis Bitdefender die Systemoptimierung abgeschlossen hat.

c. **Probleme**

Hier können Sie das Ergebnis der Operation sehen.

Klicken Sie auf die Schaltfläche **AUSFÜHRLICHEN BERICHT ANZEIGEN**, um umfassende Informationen zum Optimierungsprozess zu erhalten.

## 5.1.2. Optimieren der Systemstartzeit

Eine zu lange Systemstartzeit wird durch Anwendungen verursacht, die unnötigerweise ausgeführt werden, und kann zu einem echten Problem werden. Minutenlanges Warten auf den Systemstart kostet Sie wertvolle Zeit und beeinträchtigt Ihre Produktivität.

Im Fenster der Systemstartoptimierung werden alle Anwendungen angezeigt, die beim Systemstart ausgeführt werden. Hier können Sie auch ihr Verhalten festlegen.

So können Sie den Prozess für die Systemstartoptimierung starten:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf die Schaltfläche **Systemstartoptimierung**.

   a. **Anwendungen auswählen**

   Hier sehen Sie eine Liste der Anwendungen, die beim Systemstart ausgeführt werden. Wählen Sie die Anwendungen aus, die Sie deaktivieren oder beim Systemstart verzögern wollen.

b. **Auswahl anderer Nutzer**

Erfahren Sie, welche Auswahl andere Bitdefender-Benutzer für die ausgewählte Anwendung getroffen haben.

c. **Systemstartzeit**

Überprüfen Sie den Regler oben im Fenster, um die Zeit anzuzeigen, die Ihr System und die ausgewählten Anwendungen beim Start benötigen.

Ein Systemneustart ist erforderlich, um die Informationen zur Startzeit von System und Anwendungen einzuholen.

d. **Systemstart-Status**

- **Aktivieren.** Wählen Sie diese Option aus, wenn eine Anwendung beim Systemstart ausgeführt werden soll. Die Option ist standardmäßig aktiviert.
- **Verzögern.** Wählen Sie diese Option aus, um die Programmausführung beim Systemstart zu verschieben. Das bedeutet, dass die ausgewählten Anwendungen nach der Anmeldung des Benutzers am System mit einer fünfminütigen Verzögerung gestartet werden. Die **Verzögern**-Funktion ist vordefiniert und kann nicht vom Benutzer konfiguriert werden.
- **Deaktivieren.** Wählen Sie diese Option aus, um die Programmausführung beim Systemstart zu deaktivieren.

e. **Bericht**

Informationen wie die geschätzte Systemstartzeit nach Verzögerung oder Deaktivierung von Programmen wird angezeigt.

Das System muss eventuell neu gestartet werden, um alle Informationen anzuzeigen.

Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

### Beachten Sie

Falls Ihre Lizenz ausläuft oder Sie sich entscheiden, Bitdefender zu deinstallieren, werden die Starteinstellungen für die Programme, die Sie von der Ausführung beim Systemstart ausgenommen haben, auf den Standard zurückgesetzt.

## 5.1.3. Optimierung Ihrer Festplatte

Nicht benötigte Dateien und Ordner, die Speicherplatz auf Ihrer Festplatte belegen, können das System verlangsamen. Darum sollten Sie Ihr System zur Verbesserung der Geschwindigkeit regelmäßig bereinigen.

Mit Bitdefender Disk Cleanup hilft Ihnen bei der Optimierung von Speicherplatz, indem es Dateien findet, die möglicherweise für Ihr Speicherplatzproblem verantwortlich sind. Sie können zudem selbst entscheiden, wie mit den gefundenen Dateien verfahren werden soll.

So beginnen Sie mit der Bereinigung Ihres Systems:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf die **Disk Cleanup**-Schaltfläche.
3. Beim ersten Aufrufen von Disk Cleanup werden Sie mit der Funktion vertraut gemacht. Klicken zum Fortfahren auf **OK, VERSTANDEN**.

   a. **Laufwerke und Geräte**

      Es wird eine Liste mit allen verfügbaren Festplatten angezeigt. Neben den Windows-Festplatten werden auch externe Festplatten und USB-Geräte geprüft und in der Liste angezeigt. Klicken Sie in dem Laufwerksbereich, den Sie bereinigen wollen, auf **LAUFWERK ANALYSIEREN**.

   b. **Laufwerk wird analysiert**

      Das ausgewählte Laufwerk wird analysiert. Bitte warten Sie, bis Bitdefender die Suche nach großen Dateien und Ordnern beendet hat.

   c. **Probleme**

      Hier können Sie die Ergebnisse der Operation sehen. Nutzen Sie den **SORTIEREN NACH**-Dropdownpfeil links im Fenster, um die Reihenfolge der angezeigten Ergebnisse festzulegen. Sie können die Ergebnisse nach Dateigröße (von 10 MB bis über 5 GB) oder nach Dateityp (dabei werden die Dateien je nach Erweiterung in getrennten Ordner angezeigt) sortieren.

      Wählen Sie die zu löschenden Dateien aus und klicken Sie danach auf **AUSWAHL BESTÄTIGEN**, um den Löschvorgang zu starten.

Geschützte und für den Betrieb Ihres Systems benötigte Dateien werden ebenfalls gefunden, können aber nicht ausgewählt oder gelöscht werden.

Klicken Sie auf das -Symbol, um die Ordner aufzurufen, in denen die ausgewählten Dateien abliegen.

d. **Bestätigen Sie Ihre Auswahl**

Eine Liste mit allen ausgewählten Dateien wird angezeigt. Sehen Sie sich die Liste noch einmal an und prüfen Sie, ob Sie diese Dateien wirklich nicht benötigen, da es nicht möglich ist, diese nach dem nächsten Schritt aus dem Papierkorb wiederherzustellen. Bestätigen Sie Ihre Auswahl, indem Sie auf **LÖSCHEN** klicken.

e. **Ergebnisübersicht**

Der Vorgangsstatus wird wie folgt angezeigt:

Alle ausgewählten Dateien wurden gelöscht.
Eine oder mehrere der ausgewählten Dateien konnten nicht gelöscht werden **oder** keine der ausgewählten Dateien konnte gelöscht werden.

Klicken Sie auf **Beenden**, um das Fenster zu schließen.

## 5.2. Profile

Das Arbeiten, Filme schauen oder Spielen am Computer kann das System verlangsamen, ganz besonders dann, wenn diese Aktivitäten mit Windows-Update-Vorgängen oder Wartungsaufgaben einhergehen. Mit Bitdefender können Sie jetzt ein bevorzugtes Profil auswählen und anwenden und damit Ihr System so anpassen, dass die jeweils benötigten Anwendungen optimal laufen.

Bitdefender bietet die folgenden Profile:

- Arbeitsprofil
- Filmprofil
- Spielprofil
- Öffentliches WLAN-Profil
- Akkubetriebsprofil

Falls Sie sich entscheiden, die **Profile** nicht zu nutzen, wird ein voreingestelltes Profil mit dem Namen **Standard** aktiviert, dass Ihr System nicht optimiert.

In Übereinstimmung mit Ihrer Aktivität werden die folgenden Produkteinstellungen vorgenommen, wenn ein Arbeits-, Film- oder Spielprofil aktiviert wird:

- Alle Bitdefender-Alarme und Pop-ups sind deaktiviert.
- Automatische Updates werden verschoben.
- Geplante Scans werden verschoben.
- Das Spam-Schutz-Funktion ist aktiviert.
- Der Suchberater wird deaktiviert.
- Benachrichtigungen zu Sonderangeboten sind deaktiviert.

In Übereinstimmung mit Ihrer Aktivität werden die folgenden Systemeinstellungen vorgenommen, wenn ein Arbeits-, Film- oder Spielprofil aktiviert wird:

- Automatische Windows-Updates werden verschoben.
- Windows-Benachrichtigungen und Pop-ups sind deaktiviert.
- Nicht benötigte Hintergrundprogramme werden angehalten.
- Die visuellen Effekte werden für maximale Leistung optimiert.
- Wartungsaufgaben werden verschoben.
- Die Energiespareinstellungen werden angepasst.

Bei Aktivierung das Öffentlichen-WLAN-Profils werden von Bitdefender Total Security 2018 automatisch die folgenden Programmeinstellungen vorgenommen:

- Die Erweiterte Gefahrenabwehr ist aktiviert
- Die Bitdefender-Firewall ist aktiviert und die folgenden Einstellungen werden auf Ihren Drahtlosadapter angewandt.
  - Tarnkappe - AKTIVIERT
  - Netzwerktyp - Öffentlich
- Die folgenden Einstellungen des Internet-Schutzes werden aktiviert:

- SSL scannen
- Schutz gegen Betrug
- Schutz vor Phishing-Attacken

### 5.2.1. Arbeitsprofil

Das gleichzeitige Ausführen von verschiedenen Aufgaben bei der Arbeit am PC, so zum Beispiel das Versenden von E-Mails, das Abhalten von Videokonferenzen mit Kollegen oder das Arbeiten mit Grafikprogrammen, können die Leistung Ihres Systems beeinträchtigen. Das Arbeitsprofil wurde entwickelt, um Sie effizienter arbeiten zu lassen. Dafür werden einige Hintergrunddienste und Wartungsaufgaben deaktiviert.

#### Konfigurieren des Arbeitsprofils

So konfigurieren Sie die durchzuführenden Aktionen für das Arbeitsprofil:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das ⚙-Symbol.
2. Wechseln Sie zum Reiter **PROFILE**.
3. Klicken Sie im Bereich Arbeitsprofil auf **KONFIGURIEREN**.
4. Wählen Sie die Systemanpassungen aus, die Sie durchführen möchten, indem Sie die folgenden Optionen auswählen:
   - Die Systemleistung für Arbeitsanwendungen steigern
   - Produkteinstellungen für das Arbeitsprofil optimieren
   - Hintergrundprogramme und Wartungsaufgaben verschieben
   - Automatische Windows-Updates später durchführen
5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Fenster zu schließen.

#### Manuelles Hinzufügen von Anwendungen zur Arbeitsprofilliste

Wenn das Arbeitsprofil im Bitdefender beim Aufrufen einer Arbeitsanwendung nicht automatisch aktiviert wird, können Sie die Anwendung manuell zu der **Anwendungsliste** hinzufügen.

So fügen Sie Anwendungen manuell zur Anwendungsliste im Arbeitsprofil hinzu:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **PROFILE**.
3. Klicken Sie im Bereich Arbeitsprofil auf **KONFIGURIEREN**.
4. Klicken Sie im Fenster **ARBEITSPROFIL** auf den Link zur **Anwendungsliste**.
5. Klicken Sie auf **Hinzufügen**, um eine neue Anwendung zur **Anwendungsliste** hinzuzufügen.

   Ein neues Fenster wird angezeigt. Scrollen Sie bitte bis zu der ausführbaren Datei der Anwendung, wählen Sie diese aus und klicken Sie auf **OK**, um diese zu der Liste hinzuzufügen.

## 5.2.2. Filmprofil

Das Abspielen von Videos mit hoher Qualität, so zum Beispiel HD-Filme, nimmt viele Systemressourcen in Anspruch. Mit dem Filmprofil werden die System- und Produkteinstellungen so angepasst, dass Sie Ihre Filme ungestört genießen können.

### Konfigurieren des Filmprofils

So konfigurieren Sie die durchzuführenden Aktionen für das Filmprofil:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **PROFILE**.
3. Klicken Sie im Bereich Filmprofil auf **KONFIGURIEREN**.
4. Wählen Sie die Systemanpassungen aus, die Sie durchführen möchten, indem Sie die folgenden Optionen auswählen:
   - Die Systemleistung für das Abspielen von Videos steigern
   - Produkteinstellungen für das Filmprofil optimieren
   - Hintergrundprogramme und Wartungsaufgaben verschieben
   - Automatische Windows-Updates später durchführen

- Energiesparplaneinstellungen für den Filmbetrieb anpassen

5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Fenster zu schließen.

### Manuelles Hinzufügen von Video-Playern zur Filmprofilliste

Wenn das Filmprofil im Bitdefender beim Aufrufen eines Video-Players nicht automatisch aktiviert wird, können Sie den Player manuell zu der **Player-Liste** hinzufügen.

So fügen Sie Video-Player manuell zur Player-Liste im Filmprofil hinzu:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **PROFILE**.
3. Klicken Sie im Bereich Filmprofil auf **KONFIGURIEREN**.
4. Klicken Sie im Fenster **FILMPROFIL** auf den Link zur **Player-Liste**.
5. Klicken Sie auf **Hinzufügen**, um eine neue Anwendung zur **Player-Liste** hinzuzufügen.

   Ein neues Fenster wird angezeigt. Scrollen Sie bitte bis zu der ausführbaren Datei der Anwendung, wählen Sie diese aus und klicken Sie auf **OK**, um diese zu der Liste hinzuzufügen.

## 5.2.3. Spielprofil

Um Ihre Spiele ohne Unterbrechungen genießen zu können, müssen die Systemlast und Leistungseinbußen unbedingt minimiert werden. Durch die Kombination von verhaltensbasierten Heuristiken und einer Liste bekannter Spiele kann Bitdefender automatisch erkennen, ob ein Spiel ausgeführt wird, und Ihre Systemressourcen so optimieren, dass Sie in Ruhe spielen können.

### Konfigurieren des Spielprofils

So können Sie die durchzuführenden Aktionen für das Spielprofil konfigurieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **PROFILE**.

3. Klicken Sie im Bereich Spielprofil auf **KONFIGURIEREN**.
4. Wählen Sie die Systemanpassungen aus, die Sie durchführen möchten, indem Sie die folgenden Optionen auswählen:
   - Die Systemleistung für Spiele steigern
   - Produkteinstellungen für das Spielprofil optimieren
   - Hintergrundprogramme und Wartungsaufgaben verschieben
   - Automatische Windows-Updates später durchführen
   - Energiesparplaneinstellungen für den Spielbetrieb anpassen
5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Fenster zu schließen.

### Spiele manuell zu der Spielliste hinzufügen

Wenn das Spielprofil im Bitdefender beim Aufrufen eines Spiels oder einer Anwendung nicht automatisch aktiviert wird, können Sie die Anwendung manuell zu der **Spieleliste** hinzufügen.

So fügen Sie Spiele manuell zur Spieleliste im Spielprofil hinzu:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **PROFILE**.
3. Klicken Sie im Bereich Spielprofil auf **KONFIGURIEREN**.
4. Klicken Sie im Fenster **SPIELPROFIL** auf den Link zur **Spieleliste**.
5. Klicken Sie auf **Hinzufügen**, um ein neues Spiel zur **Spieleliste** hinzuzufügen.

   Ein neues Fenster wird angezeigt. Öffnen Sie den Ordner, in dem sich die ausführbare Datei des Spiels befindet, markieren Sie sie und klicken Sie auf **OK**, um das Spiel zur Liste hinzuzufügen.

## 5.2.4. Öffentliches WLAN-Profil

Bei Verbindungen mit unsicheren WLAN-Netzwerken kann der Versand von E-Mails, die Eingabe von sensiblen Anmeldedaten oder das Einkaufen im Internet die Vertraulichkeit Ihrer Daten gefährden. Das Öffentliche-WLAN-Profil passt die Produkteinstellungen entsprechend an, um Ihnen eine geschützte

Umgebung für Online-Zahlungen und die Eingabe von sensiblen Daten zu ermöglichen.

### Konfiguration des Öffentlichen-WLAN-Profils

So können Sie Bitdefender konfigurieren, damit die Produkteinstellungen bei Verbindungen mit unsicheren WLAN-Netzwerken entsprechend angepasst werden:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **PROFILE**.
3. Klicken Sie im Bereich Öffentliches-WLAN-Profil auf **KONFIGURIEREN**.
4. Lassen Sie das Kästchen **Passt Produkteinstellungen so an, dass bei Einwahl in ein ungeschütztes WLAN-Netzwerk der Schutz erhöht wird** aktiviert.
5. Klicken Sie auf **Speichern**.

## 5.2.5. Akkubetriebsprofil

Das Profil für den Akkubetrieb wurde speziell für Laptop- und Tablet-Nutzer entwickelt. Er minimiert die Auswirkungen des System- und Bitdefender-Betriebs auf die Akkulaufzeit, sobald der von Ihnen oder standardmäßig festgelegte Akkuladestand unterschritten wird.

### Konfiguration des Profils für den Akkubetrieb

So konfigurieren Sie das Profil für den Akkubetrieb:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **PROFILE**.
3. Klicken Sie im Bereich Akkubetriebsprofil auf **KONFIGURIEREN**.
4. Wählen Sie die durchzuführenden Systemanpassungen aus, indem Sie die folgenden Optionen auswählen:
   - Produkteinstellungen für den Akkubetrieb optimieren.
   - Hintergrundprogramme und Wartungsaufgaben verschieben.

- Automatische Windows-Updates später durchführen.
- Energiesparplaneinstellungen für den Akkubetrieb anpassen.
- Externe Geräte und Netzwerk-Ports deaktivieren.

5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Fenster zu schließen.

Geben Sie einen gültigen Wert in das Drehfeld ein oder wählen Sie ihn über die Pfeiltasten aus, um festzulegen, wann das System in den Akkubetrieb wechseln soll. Standardmäßig wird der Akkubetrieb aktiviert, sobald der Akkuladestand unter 30 % sinkt.

Die folgenden Produkteinstellungen werden angewendet, wenn Bitdefender in das Akkubetriebsprofil versetzt wird:

- Automatische Bitdefender-Updates werden verschoben.
- Geplante Scans werden verschoben.
- Das Sicherheits-Widget wird deaktiviert.

Bitdefender erkennt, wenn Ihr Laptop vom Stromnetz getrennt wird und startet den Akkubetrieb automatisch je nach festgelegten Akkuladestand. Ebenso beendet Bitdefender automatisch den Akkubetrieb, wenn der Laptop nicht mehr über den Akku betrieben wird.

## 5.2.6. Echtzeitoptimierung

Die Bitdefender-Echtzeitoptimierung ist ein Plug-in, das Ihre Systemleistung unbemerkt im Hintergrund verbessert und so sicherstellt, dass Sie im Profile-Modus nicht gestört werden. Je nach CPU-Auslastung überwacht das Plug-in alle Prozesse und konzentriert sich dabei auf Prozesse, die Ihr System überdurchschnittlich belasten, um sie an Ihre Anforderungen anzupassen.

So können Sie die Echtzeitoptimierung aktivieren oder deaktivieren:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das ⚙-Symbol.
2. Wechseln Sie zum Reiter **PROFILE**.
3. Scrollen Sie nach unten bis zur Option Echtzeitoptimierung und klicken Sie zur Aktivierung oder Deaktivierung auf den entsprechenden Schalter.

# 6. PROBLEMLÖSUNG

## 6.1. Verbreitete Probleme beheben

In diesem Kapitel werden einige Probleme, die Ihnen bei der Verwendung von Bitdefender begegnen können, erläutert. Zudem finden Sie hier Lösungsvorschläge für diese Probleme. Die meisten dieser Probleme können über eine passende Konfiguration der Produkteinstellungen gelöst werden.


- *„Mein System scheint langsamer zu sein“* (S. 200)
- *„Der Scan startet nicht“* (S. 202)
- *„Ich kann eine App nicht mehr verwenden“* (S. 204)
- *„Wie gehe ich vor, wenn Bitdefender eine sichere Website oder Online-Anwendung blockiert?“* (S. 205)
- *„Wie gehe ich vor, wenn Bitdefender eine sichere Anwendung als Ransomware einstuft?“* (S. 206)
- *„Wie man Bitdefender-Updates auch mit einer langsamen Internet-Verbindung durchführen kann“* (S. 211)
- *„Bitdefender-Dienste antworten nicht“* (S. 212)
- *„Der Spam-Schutz-Filter funktioniert nicht richtig“* (S. 212)
- *„Das automatische Einfügen funktioniert bei meiner Geldbörse nicht“* (S. 218)
- *„Entfernen von Bitdefender ist fehlgeschlagen“* (S. 219)
- *„Mein System fährt nach der Installation von Bitdefender nicht mehr hoch“* (S. 220)


Wenn Sie Ihr Problem hier nicht finden oder wenn die vorgeschlagene Lösung nicht zum Erfolg führt, können Sie den technischen Kundendienst von Bitdefender wie in Kapitel *„Hilfe anfordern“* (S. 341) beschrieben, kontaktieren.

### 6.1.1. Mein System scheint langsamer zu sein

Nach der Installation einer Sicherheitssoftware ist eine geringfügige Verlangsamung des Systems bis zu einem gewissen Grad normal.

Wenn Sie eine erhebliche Systemverlangsamung feststellen, kann dies folgende Ursachen haben:

- **Bitdefender ist nicht die einzige auf Ihrem System installierte Sicherheits-Software.**

  Obwohl Bitdefender bereits auf Ihrem System installierte Sicherheitsprogramme während der Installation sucht und entfernt, empfehlen wir dennoch, jede andere Sicherheitslösung von Ihrem Rechner zu entfernen, bevor Sie die Installation von Bitdefender starten. Weitere Informationen finden Sie unter *„Wie entferne ich andere Sicherheitslösungen?“ (S. 87)*.

- **Die Mindestsystemanforderungen für die Ausführung von Bitdefender sind nicht erfüllt.**

  Wenn Ihr PC die Mindestsystemanforderungen nicht erfüllt, verlangsamt dies Ihr System, insbesondere dann, wenn mehrere Anwendungen gleichzeitig laufen. Weitere Informationen finden Sie unter „Mindestsystemanforderungen“ (S. 3).

- **Sie haben Apps installiert, die Sie nicht verwenden**.

  Ein beliebiger Computer hat Programme oder Apps, die Sie nicht verwenden. Im Hintergrund laufen viele unerwünschte Programme, die Speicherplatz und Arbeitsspeicher beanspruchen. Wenn Sie ein Programm nicht nutzen, deinstallieren Sie es. Das gilt auch für vorinstallierte Software oder Testversionen, die Sie nicht wieder entfernt haben.

  Wichtig

  Wenn Sie glauben, dass ein Programm oder eine Anwendung ein wichtiger Bestandteil Ihres Betriebssystems ist, entfernen Sie es nicht und wenden Sie sich an den Bitdefender-Kundendienst.

- **Ihr System ist vielleicht infiziert**.

  Die Geschwindigkeit und das allgemeine Verhalten Ihres Systems kann auch durch Bedrohungen beeinträchtigt werden. Spyware, Malware, Trojaner und Adware wirken sich negativ auf Ihre Systemleistung aus. Stellen Sie sicher, dass Ihr System regelmäßig gescannt wird, mindestens einmal pro Woche. Es empfiehlt sich, einen Bitdefender-System-Scan durchzuführen, da so nach allen Bedrohungsarten gesucht wird, die die Sicherheit Ihres Systems gefährden.

  So können Sie einen System-Scan starten:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **VIRENSCHUTZ** auf **System-Scan**.
4. Befolgen Sie die Anweisungen des Assistenten.

### 6.1.2. Der Scan startet nicht

Dieses Problem kann folgende Ursachen haben:

- **Eine vorherige Installation von Bitdefender wurde nicht vollständig entfernt oder es handelt sich um eine fehlerhafte Bitdefender-Installation**.

  Installieren Sie Bitdefender in diesem Fall neu:

  - In **Windows 7**:
    1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
    2. Suchen Sie **Bitdefender Total Security 2018** und wählen Sie **Deinstallieren**.
    3. Klicken Sie im angezeigten Fenster auf **NEU INSTALLIEREN**.
    4. Warten Sie, bis die Neuinstallation abgeschlossen ist und starten Sie Ihr System neu.
  - In **Windows 8 und Windows 8.1**:
    1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
    2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
    3. Suchen Sie **Bitdefender Total Security 2018** und wählen Sie **Deinstallieren**.
    4. Klicken Sie im angezeigten Fenster auf **NEU INSTALLIEREN**.
    5. Warten Sie, bis die Neuinstallation abgeschlossen ist und starten Sie Ihr System neu.
  - In **Windows 10**:

1. Klicken Sie auf **Start** und danach auf Einstellungen.
2. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie danach auf **Installierte Anwendungen**.
3. Suchen Sie **Bitdefender Total Security 2018** und wählen Sie **Deinstallieren**.
4. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.
5. Klicken Sie im angezeigten Fenster auf **NEU INSTALLIEREN**.
6. Warten Sie, bis die Neuinstallation abgeschlossen ist und starten Sie Ihr System neu.

**Beachten Sie**

Wenn Sie bei der Neuinstallation wie hier beschrieben vorgehen, werden Ihre benutzerdefinierte Einstellungen gespeichert und sind im neu installierten Produkt wieder verfügbar. Weitere Einstellungen werden unter Umständen wieder auf die Standardkonfiguration zurückgesetzt.

- **Bitdefender ist nicht die einzige auf Ihrem System installierte Sicherheits-Software**.

  In diesem Fall:

  1. Entfernen Sie die andere Sicherheitslösung. Weitere Informationen finden Sie unter *„Wie entferne ich andere Sicherheitslösungen?“* (S. 87).
  2. Bitdefender neu installieren:
     - In **Windows 7**:
       a. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
       b. Suchen Sie **Bitdefender Total Security 2018** und wählen Sie **Deinstallieren**.
       c. Klicken Sie im angezeigten Fenster auf **NEU INSTALLIEREN**.
       d. Warten Sie, bis die Neuinstallation abgeschlossen ist und starten Sie Ihr System neu.
     - In **Windows 8 und Windows 8.1**:
       a. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.

b. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.

c. Suchen Sie **Bitdefender Total Security 2018** und wählen Sie **Deinstallieren**.

d. Klicken Sie im angezeigten Fenster auf **NEU INSTALLIEREN**.

e. Warten Sie, bis die Neuinstallation abgeschlossen ist und starten Sie Ihr System neu.

- In **Windows 10**:

a. Klicken Sie auf **Start** und danach auf Einstellungen.

b. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie danach auf **Installierte Anwendungen**.

c. Suchen Sie **Bitdefender Total Security 2018** und wählen Sie **Deinstallieren**.

d. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.

e. Klicken Sie im angezeigten Fenster auf **NEU INSTALLIEREN**.

f. Warten Sie, bis die Neuinstallation abgeschlossen ist und starten Sie Ihr System neu.

**Beachten Sie**

Wenn Sie bei der Neuinstallation wie hier beschrieben vorgehen, werden Ihre benutzerdefinierte Einstellungen gespeichert und sind im neu installierten Produkt wieder verfügbar. Weitere Einstellungen werden unter Umständen wieder auf die Standardkonfiguration zurückgesetzt.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“ (S. 341)* beschrieben.

### 6.1.3. Ich kann eine App nicht mehr verwenden

Dieses Problem tritt auf, wenn Sie versuchen, ein Programm zu verwenden, das vor der Installation von Bitdefender einwandfrei funktioniert hatte.

Nach der Installation von Bitdefender könnten folgende Situationen eintreten:

- Sie könnten einen Benachrichtigung von Bitdefender erhalten, dass das Programm versucht, Veränderungen am System durchzuführen.

- Es ist möglich, dass Sie von dem Programm, das Sie starten möchten, eine Fehlermeldung erhalten.

Diese Situation tritt ein, wenn die Erweiterte Gefahrenabwehr eine Anwendung fälschlicherweise als Malware einstuft.

Die Erweiterte Gefahrenabwehr ist ein Bitdefender-Modul, das alle laufenden Anwendungen auf Ihren Systemen durchgehend überwacht und einen Bericht über jene sendet, die sich potenziell gefährlich verhalten. Da diese Funktion auf einem heuristischen System basiert, kann es dazu kommen, dass auch seriöse Anwendungen im Bericht der Erweiterten Gefahrenabwehr aufgelistet werden.

In solchen Fällen können Sie die entsprechende Anwendung von der Überwachung durch die Erweiterte Gefahrenabwehr ausschließen.

So können Sie das Programm zur Ausschlussliste hinzufügen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **ADVANCED THREAT DEFENSE**.
4. Klicken Sie im Fenster **WHITELIST** auf **Anwendungen zur Whitelist hinzufügen**.
5. Suchen Sie die Anwendung, die ausgeschlossen werden soll, und klicken Sie auf **OK**.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“ (S. 341)* beschrieben.

## 6.1.4. Wie gehe ich vor, wenn Bitdefender eine sichere Website oder Online-Anwendung blockiert?

Bitdefender ermöglicht Ihnen sicheres Surfen im Netz, indem es den Internet-Datenverkehr filtert und schädliche Inhalte blockiert. Es kann jedoch auch vorkommen, dass Bitdefender eine sichere Website oder Online-Anwendung als unsicher einstuft, wodurch diese dann durch den Bitdefender-Scan des HTTP-Datenverkehrs irrtümlich blockiert werden.

Sollte die gleiche Seite oder Anwendung wiederholt blockiert werden, können Sie diese zu einer sogenannten Whitelist hinzufügen, damit sie von den Bitdefender-Engines nicht mehr gescannt werden. So können Sie ungestört im Internet surfen.

So können Sie eine Website zur **Whitelist** hinzufügen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **INTERNET-SCHUTZ** auf **Whitelist**.
4. Geben Sie die Adresse der blockierten Website oder Online-Anwendung in das entsprechende Feld ein und klicken Sie **Hinzufügen**.
5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Fenster zu schließen.

Sie sollten dieser Liste nur Websites und Anwendungen hinzufügen, denen Sie auch wirklich vertrauen. Diese werden dann von den folgenden Engines vom Scan ausgeschlossen: Bedrohung, Phishing und Betrug.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“ (S. 341)* beschrieben.

### 6.1.5. Wie gehe ich vor, wenn Bitdefender eine sichere Anwendung als Ransomware einstuft?

Bei Ransomware handelt es sich um schädliche Programme, die anfällige Systeme für den Benutzer sperren und für deren Freigabe Lösegeld erpressen. Um Ihr System vor ungünstigen Situationen zu schützen, können Sie Ihre persönlichen Dateien mit Bitdefender absichern.

Versucht eine Anwendung, eine Ihrer geschützten Dateien zu verändern oder zu löschen, wird diese als unsicher eingestuft und Bitdefender wird alle Funktionen der Anwendung blockieren.

Falls eine solche App zur Liste der nicht vertrauenswürdigen Apps hinzugefügt wurde und Sie sich sicher sind, dass eine Nutzung kein Risiko darstellt, gehen Sie folgendermaßen vor:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.

2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **SICHERE DATEIEN** auf **Anwendungszugriff**.
4. Hier werden alle Anwendungen aufgelistet, die versucht haben, Dateien in Ihren geschützten Ordnern zu verändern. Klicken Sie auf Zulassen und wählen Sie die Anwendung aus, die Sie als sicher einstufen.

## 6.1.6. Ich kann keine Verbindung zum Internet herstellen

Nach der Installation von Bitdefender werden Sie unter Umständen bemerken, dass ein Programm oder ein Browser keine Verbindung mehr zum Internet herstellen oder auf Netzwerkdienste zugreifen kann.

In diesem Fall ist es die beste Lösung, Bitdefender so zu konfigurieren, dass Verbindungen von und zu der jeweiligen Software-Anwendung automatisch zugelassen werden:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **FIREWALL**.
4. Wechseln Sie zum Reiter **REGELN**.
5. Klicken Sie auf die Link **Regel hinzufügen**, um eine Anwendungsregel hinzuzufügen.
6. Ein neues Fenster wird angezeigt, in dem Sie die Details hinzufügen können. Stellen Sie sicher, dass Sie alle verfügbaren Netzwerktypen auswählen und klicken Sie im Bereich **Berechtigung** auf **Zulassen**.

Schließen Sie Bitdefender, öffnen Sie die Software-Anwendung und versuchen Sie erneut, eine Verbindung mit dem Internet aufzubauen.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“* (S. 341) beschrieben.

## 6.1.7. Ich kann auf ein Gerät in meinem Netzwerk nicht zugreifen

Abhängig von dem Netzwerk mit dem Sie verbunden sind, könnte die Bitdefender-Firewall die Verbindung zwischen Ihrem System und einem anderen Gerät (zum Beispiel einem anderen Computer oder Drucker)

blockieren. Dadurch sind Sie vielleicht nicht mehr in der Lage, Dateien auszutauschen oder zu drucken.

In diesem Fall ist es die beste Lösung, Bitdefender so zu konfigurieren, dass Verbindungen von und zu dem jeweiligen Gerät automatisch zugelassen werden. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie auf das -Symbol unten rechts im Bereich **FIREWALL**.
4. Klicken Sie oben im Fenster **REGELN** auf **Regel hinzufügen**.
5. Aktivieren Sie im Fenster **EINSTELLUNGEN** die Option **Diese Regel auf alle Anwendungen anwenden**.
6. Wechseln Sie zum Reiter **ERWEITERT**.
7. Geben Sie im Feld **Benutzerdefinierte Remoteadresse** die IP-Adresse des Computers oder Druckers ein, auf den Sie uneingeschränkten Zugriff haben möchten.

Wenn eine Verbindung mit dem Gerät immer noch nicht möglich ist, wird das Problem vielleicht nicht durch Bitdefender hervorgerufen.

Überprüfen Sie andere mögliche Ursachen, wie z.B:

- Die Firewall auf dem anderen Computer könnte die Nutzung des gemeinsamen Druckers oder der Datei blockieren.
  - Wenn die Windows Firewall genutzt wird, kann diese wie folgt zum Zulassen von Datei- und Druckerfreigabe konfiguriert werden:
    - In **Windows 7**:
      1. Klicken Sie auf **Start**, öffnen Sie die **Systemsteuerung** und wählen Sie **System und Sicherheit**.
      2. Öffnen Sie die **Windows-Firewall** und wählen Sie dann **Programm durch die Windows-Firewall kommunizieren lassen**.
      3. Wählen Sie die Option **Datei- und Druckerfreigabe**.
    - In **Windows 8 und Windows 8.1**:

1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
2. Klicken Sie auf **System und Sicherheit**, öffnen Sie die **Windows-Firewall** und wählen Sie **Apps über die Windows-Firewall kommunizieren lassen**.
3. Wählen Sie die Option **Datei- und Druckerfreigabe** aus und klicken Sie **OK**.

- In **Windows 10**:
  1. Geben Sie "Apps über die Windows-Firewall kommunizieren lassen" in das Suchfeld in der Taskleiste ein und klicken Sie auf das entsprechende Symbol.
  2. Klicken Sie auf **Einstellungen ändern**.
  3. Wählen Sie in der Liste der **Zugelassenen Apps und Features** die Option **Datei- und Druckerfreigabe** aus und klicken Sie **OK**.
- Wenn eine andere Firewall verwendet wird, greifen Sie bitte auf die entsprechende Dokumentation oder Hilfedatei zurück.

- Allgemeine Umstände, die eine Benutzung des oder Verbindung mit dem freigegebenen Drucker verhindern könnten:
  - Möglicherweise müssen Sie sich als Windows-Administrator anmelden, um auf den freigegebenen Drucker zugreifen zu können.
  - Für den gemeinsam genutzten Drucker werden Rechte vergeben, so dass dieser nur bestimmten Computern und Benutzern den Zugriff erlaubt. Falls Sie Ihren Drucker zur gemeinsamen Nutzung freigegeben haben, überprüfen Sie die Rechte, die für den Drucker vergeben wurden, um festzustellen, ob der Nutzer des anderen Computers Zugriffsrechte erhalten hat. Wenn Sie versuchen, eine Verbindung zu einem freigegebenen Drucker aufzubauen, sollten Sie mit Benutzer auf dem anderen Computer abklären, ob Sie die benötigten Rechte haben.
  - Der Drucker, der mit Ihren Computer oder dem anderen Computer verbunden ist, ist nicht freigegeben.
  - Der freigegebene Drucker wurde dem Computer nicht hinzugefügt.

> **Beachten Sie**
> Um mehr darüber zu erfahren, wie Sie die Druckerfreigabe verwalten können (Drucker freigeben, Rechte vergeben oder entziehen, Verbindungen mit einen freigegebenen Drucker herstellen), klicken sie im Windows-Startmenü auf **Hilfe und Support**).

- Der Zugriff auf einen Netzwerk-Drucker könnte auf bestimmte Computer oder Nutzer beschränkt sein. Fragen Sie Ihren Netzwerk-Administrator, ob Sie die notwendigen Rechte besitzen, um auf diesen Drucker zuzugreifen.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“ (S. 341)* beschrieben.

## 6.1.8. Meine Internetverbindung ist langsam

Diese Situation könnte nach der Installation von Bitdefender eintreten. Das Problem könnte aufgrund von Konfigurationsfehlern der Bitdefender-Firewall auftreten.

So können Sie das Problem behandeln:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **FIREWALL** auf den EIN/AUS-Schalter, um die Funktion zu deaktivieren.
4. Überprüfen Sie, ob Sie nach der Deaktivierung der Bitdefender-Firewall eine Verbesserung der Internet-Verbindung feststellen können.
   - Wenn die Internetverbindung immer noch langsam ist, wird das Problem vielleicht nicht durch Bitdefender hervorgerufen. Sie sollten Ihren Internet-Provider kontaktieren, um abzuklären, dass es von seiner Seite aus keine Verbindungsprobleme gibt.

     Wenn Sie von Ihrem Internet-Anbieter die Bestätigung erhalten, dass es auf Anbieterseite keine Probleme gibt und das Problem besteht weiterhin, kontaktieren Sie Bitdefender wie im Abschnitt *„Hilfe anfordern“ (S. 341)* beschrieben.
   - Falls Sie nach der Deaktivierung der Bitdefender-Firewall eine Verbesserung der Internet-Verbindung feststellen können:

a. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.

b. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.

c. Klicken Sie auf das -Symbol unten rechts im Bereich **FIREWALL**.

d. Wechseln Sie zum Reiter **NETZWERKADAPTER** und legen Sie Ihre Internetverbindung als **Heim/Büro** fest.

e. Klicken Sie im Reiter **ERWEITERTE EINSTELLUNGEN** auf den Schalter, um **Port-Scans im Netzwerk blockieren** zu deaktivieren.

Klicken Sie im Bereich **Tarnkappe** auf **Tarneinstellungen bearbeiten**. Aktivieren Sie die Tarnkappe für den Netzwerkadapter, mit dem Sie verbunden sind.

f. Schließen Sie Bitdefender, starten Sie das System neu und überprüfen Sie die Internet-Verbindungsgeschwindigkeit.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“ (S. 341)* beschrieben.

## 6.1.9. Wie man Bitdefender-Updates auch mit einer langsamen Internet-Verbindung durchführen kann

Falls Sie über eine langsame Internet-Verbindung (wie z. B. ein Modem) verfügen, können während des Updates Fehler auftreten.

So stellen Sie sicher, dass die Datenbank mit den Bedrohungsinformationen in Bitdefender jederzeit auf dem neuesten Stand ist:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Wechseln Sie zum Reiter **UPDATE**.
3. Wählen Sie neben **Update-Verarbeitungsregeln** den Eintrag **Vor dem Download nachfragen** aus dem Menü aus.
4. Kehren Sie zum Hauptfenster zurück und klicken Sie auf den **JETZT AKTUALISIEREN**-Link.
5. Wählen Sie nur **Signatur-Updates** und klicken Sie dann auf **OK**.
6. Bitdefender wird nur die Datenbank mit den Bedrohungsinformationen herunterladen und installieren.

## 6.1.10. Bitdefender-Dienste antworten nicht

Dieser Artikel hilft Ihnen bei der Lösung des Problems **Bitdefender-Dienste antworten nicht**. Sie könnten folgende Fehlermeldung erhalten:

- Das Bitdefender-Symbol im der Task-Leiste ist grau hinterlegt und Sie erhalten eine Meldung, dass die Bitdefender-Dienste nicht reagieren.
- Das Bitdefender-Fenster zeigt an, dass die Bitdefender-Dienste nicht antworten.

Der Fehler kann durch einen der folgenden Umstände verursacht werden:

- Temporäre Kommunikationsstörungen zwischen den Bitdefender-Diensten.
- Einige der Bitdefender-Dienste wurden angehalten.
- Andere Sicherheitslösungen laufen gleichzeitig mit Bitdefender auf Ihrem Rechner.

Um diesen Fehler zu beheben, versuchen Sie folgenden Lösungen:

1. Warten Sie einen Moment und beobachten Sie, ob sich etwas ändert. Der Fehler könnte vorübergehend sein.
2. Starten Sie den Rechner neu und warten Sie einige Momente, bis Bitdefender geladen ist. Öffnen Sie Bitdefender und überprüffen Sie ob das Problem immernoch besteht. Durch einen Neustart des Computers wird das Problem normalerweise gelöst.
3. Überprüfen Sie, ob Sie irgendeine andere Sicherheitslösung installiert haben, weil diese den Normalbetrieb von Bitdefender stören könnte. Wenn dies der Fall ist, empfehlen wir Ihnen alle anderen Sicherheitslösungen zu entfernen und Bitdefender wieder neu zu installieren.

   Weitere Informationen finden Sie unter *„Wie entferne ich andere Sicherheitslösungen?“ (S. 87)*.

Sollte der Fehler weiterhin auftreten, wenden Sie sich bitte an unsere Support-Mitarbeiter, wie in Abschnitt *„Hilfe anfordern“ (S. 341)* beschrieben.

## 6.1.11. Der Spam-Schutz-Filter funktioniert nicht richtig

Dieser Artikel hilft Ihnen, folgende Probleme mit dem Bitdefender Antispam-Filter lösen:

- Eine Anzahl von seriösen E-Mails werden markiert als [spam].

- Viele Spams werden entsprechend nicht durch den Antispam Filter markiert.
- Der Antispam-Filter entdeckt keine Spamnachrichten.

## Legitime Nachrichten werden als [spam] markiert

Seriöse Nachrichten werden als [spam] markiert, einfach deshalb weil sie für den Bitdefender Antispam-Filter wie solche aussehen. Im Normalfall können Sie dieses Problem lösen indem Sie den Antispam Filter angemessen konfigurieren.

Bitdefender fügt die Empfänger Ihrer Mails automatisch der Freundeliste hinzu. Die E-Mails, die von Kontakten in der Freunde Liste empfangen werden, werden als seriös angesehen. Sie werden nicht vom Spam-Filter geprüft und deshalb auch nie als [spam] markiert.

Die automatische Konfiguration der Freundesliste verhindert nicht die entdeckte Störungen, die in dieser Situationen auftreten können:

- Sie empfangen viele angeforderte Werb-E-Mails resultierend aus der Anmeldung auf verschiedene Webseiten. In diesem Fall ist die Lösung, die E-Mail Adressen, von denen Sie solche E-Mails bekommen, auf die Freunde Liste zu setzen.
- Ein erheblicher Teil Ihrer legitimen Email ist von Leuten, die bisher nie E-Mails von Ihnen erhalten haben. bspw. Kunden, potentielle Geschäftspartner und andere. Andere Lösungen sind in diesem Fall erforderlich.

  Wenn Sie einen der Mail-Clients nutzen, in die sich Bitdefender integriert, weisen Sie auf Erkennungsfehler hin.

  **Beachten Sie**
  Bitdefender integriert sich in die gebräuchlichsten Mail Clients durch eine einfach zu verwendende Antispam-Symbolleiste. Um die komplette Liste der unterstützen E-Mail Clients zu erhalten, lesen Sie bitte: *„Unterstützte E-Mail-Clients und Protokolle“* (S. 121).

## Kontakte zur Freundesliste hinzufügen

Wenn Sie einen unterstützten E-Mail Client verwenden, können Sie den Absernder ganz leicht zu der Freundesliste hinzufügen. Folgen Sie diesen Schritten:

1. Wählen Sie in Ihrem Mail Client eine Mail eines Senders, den Sie der Freundesliste hinzufügen möchten.
2. Klicken Sie in der Bitdefender-Spam-Schutz-Symbolleiste auf die Schaltfläche **Neuer Freund**.
3. Es kann sein das Sie die Adressen, die zur Freundesliste hinzugefügt wurden, bestätigen müssen. Wählen Sie **Diese Nachricht nicht mehr anzeigen** und klicken Sie **OK**.

Sie werden jetzt immer E-Mails von diesem Absender erhalten, egal welchen Inhalts.

Falls Sie einen anderen Mail Client verwenden, können Sie von der Bitdefender-Oberfläche aus Kontakte der Freundeliste hinzufügen. Folgen Sie diesen Schritten:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **SPAM-SCHUTZ** auf **Freunde verwalten**.

   Ein Konfigurationsfenster wird geöffnet.
4. Geben Sie die E-Mail-Adresse ein, von der Sie immer E-Mails empfangen wollen und klicken Sie auf **Hinzufügen**. Sie können beliebig viele E-Mail-Adressen hinzufügen.
5. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

## Auf Erkennungsfehler hinweisen

Wenn Sie einen unterstützten E-Mail-Client verwenden, können Sie den Spam-Filter einfach korrigieren (indem Sie angeben, welche E-Mails nicht als [spam] hätten markiert werden sollen). Dadurch wird die Effizienz des Spam-Filters verbessert. Folgen Sie diesen Schritten:

1. Öffnen Sie den Mail Client.
2. Gehen Sie zu dem Junk Mail Ordner, wo die Spam Nachrichten hin verschoben werden.
3. Wählen Sie die Nachricht, die von Bitdefender fälschlicherweise als [spam] markiert wurde, aus.

4. Klicken Sie auf **Neuer Freund** in der Bitdefender-Spam-Schutz-Symbolleiste. Klicken Sie zur Bestätigung **OK**. Sie werden jetzt immer E-Mails von diesem Absender erhalten, egal welchen Inhalts.
5. Klicken Sie in der Bitdefender-Spam-Schutz-Symbolleiste (die sich üblicherweise im oberen Teil des Mail-Client-Fensters befindet) auf die Schaltfläche **Kein Spam**. Die E-Mail wird in den Posteingangsordner verschoben.

## Eine Vielzahl von Spam-Nachrichten wird nicht erkannt

Wenn Sie viele Nachrichten erhalten, die nicht als [spam] markiert sind, konfigurieren Sie den Bitdefender Antispam-Filter, um seine Effektivität zu erhöhen.

Versuchen Sie die folgenden Lösungsansätze:

1. Wenn Sie einen der Mail-Clients nutzen, in die sich Bitdefender integriert, weisen Sie auf unerkannte Spam-Nachrichten hin.

   ### Beachten Sie

   Bitdefender integriert sich in die gebräuchlichsten Mail Clients durch eine einfach zu verwendende Antispam-Symbolleiste. Um die komplette Liste der unterstützen E-Mail Clients zu erhalten, lesen Sie bitte: *„Unterstützte E-Mail-Clients und Protokolle“* (S. 121).

2. Neuen Spammer zur Liste der Spammer hinzufügen. Die E-Mail-Nachrichten, empfangen von den Adressen aus der Spammerliste, werden automatisch als [spam] markiert.

## Auf unerkannte Spam-Nachrichten hinweisen

Wenn Sie einen unterstützten E-Mail-Client verwenden, können Sie einfach angeben, welche E-Mails als Spam hätten markiert werden sollen. Dadurch wird die Effizienz des Spam-Filters verbessert. Folgen Sie diesen Schritten:

1. Öffnen Sie den Mail Client.
2. Begeben Sie sich zum Inbox Ordner.
3. Wählen Sie die unentdeckte Spam-Nachricht.
4. Klicken Sie in der Bitdefender-Spam-Schutz-Symbolleiste (die sich üblicherweise im oberen Teil des Mail-Client-Fensters befindet) auf die

Schaltfläche **Ist Spam**. Sie werden dann sofort als [spam] markiert und in den Junk-Ordner verschoben.

## Neue Spammer zur Liste der Spammer hinzufügen

Wenn Sie einen unterstützten E-Mail Client verwenden, können Sie den Absernder der Spamnachricht ganz leicht zu der Spammerliste hinzufügen. Folgen Sie diesen Schritten:

1. Öffnen Sie den Mail Client.
2. Gehen Sie zu dem Junk Mail Ordner, wo die Spam Nachrichten hin verschoben werden.
3. Markieren Sie die Nachricht die von Bitdefender als [spam] markiert wurde.
4. Klicken Sie in der Bitdefender-Spam-Schutz-Leiste auf **Neuer Spammer**.
5. Es kann sein das Sie die Adresse bestätigen müssen, die in der Spammerliste hinzugefügt wurde. Wählen Sie **Diese Nachricht nicht mehr anzeigen** und klicken Sie **OK**.

Falls Sie einen anderen E-Mail-Client verwenden, können Sie von der Bitdefender-Oberfläche aus manuell Spammer der Liste der Spammer hinzufügen. Dies sollten Sie nur dann tun, wenn Sie bereits mehrere Spam-Nachrichten vom selben Absender erhalten haben. Folgen Sie diesen Schritten:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **SPAM-SCHUTZ** auf **Spammer verwalten**.

   Ein Konfigurationsfenster wird geöffnet.
4. Geben Sie die E-Mail-Adresse des Spammers ein und klicken Sie auf **Hinzufügen**. Sie können beliebig viele E-Mail-Adressen hinzufügen.
5. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

## Der Spam-Schutz-Filter erkennt keine Spam-Nachrichten

Wenn keine Nachrichten als [spam] markiert werden, könnte es möglicherweise am Bitdefender Antispam Fileter liegen. Vor der Fehlersuche

dieses Problems, sollten Sie sicherstellen , dass es nicht durch einen der folgenden Bedingungen verursacht wird:

- Der Spam-Schutz ist unter Umständen deaktiviert. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol und wählen Sie **FUNKTIONEN ANZEIGEN** aus, um den Status des Spam-Schutzes zu überprüfen. Klicken Sie auf das Zahnrad im Bereich **SPAM-SCHUTZ** und prüfen Sie oben im Fenster, ob die Funktion aktiviert ist.

  Falls der Spam-Schutz deaktiviert ist, so liegt hier die Ursache Ihres Problems. Klicken Sie auf den entsprechenden Schalter, um Ihren Spam-Schutz zu aktivieren.

- Der Bitdefender Antispam-Schutz ist nur für Email Clients verfügbar, die Emails über das POP3-Protokoll zu empfangen. Das bedeutet folgendes:
  - Die Email-Nachrichten, die über web-basierte Email-Dienstleistungen empfangen werden (wie Yahoo, Gmail, Hotmail oder andere) gehen nichtdurch den Bitdefender Spam-Filter.
  - Wenn Ihr Email Client konfiguriert ist, Emails unter Verwendung anderer Protokolle als POP3 zu empfangen (z.B., IMAP4), scannt der Bitdefender Antispam-Filter diese Emails nicht auf Spam-Mails.

  > **Beachten Sie**
  >
  > POP3 ist eines der am meisten benutzten Protokolle für das Downloaden der E-Mail-Nachrichten vom Mail-Server. Falls Sie das Protokoll nicht kennen, das von Ihrem E-Mail Client benutzt wird, um E-Mail Nachrichten herunterzuladen, fragen Sie die Person, die Ihren E-Mail Client konfiguriert hat.

- Bitdefender Total Security 2018 scannt keine POP3-Übertragungen von Lotus Notes.

Es könnte sein, dass das Problem durch eine Reparatur oder Neuinstallation des Produkts behoben wird. Falls Sie lieber den Bitdefender-Kundendienst kontaktieren möchten, folgen Sie der Beschreibung im Abschnitt *„Hilfe anfordern“ (S. 341)*.

## 6.1.12. Das automatische Einfügen funktioniert bei meiner Geldbörse nicht

Sie haben Ihre Online-Anmeldedaten bereits in Ihrem Bitdefender-Passwortmanager gespeichert und das automatische Einfügen funktioniert nicht. Dies geschieht in aller Regel, wenn die Erweiterung für die Bitdefender-Geldbörse in Ihrem Browser nicht installiert wurde.

Um das Problem zu beheben, gehen Sie folgendermaßen vor:

- Im **Internet Explorer:**
  1. Öffnen Sie den Internet Explorer.
  2. Klicken Sie auf Extras.
  3. Klicken Sie auf Add-Ons verwalten.
  4. Klicken Sie auf Symbolleisten und Erweiterungen.
  5. Bewegen Sie den Mauszeiger auf **Bitdefender-Geldbörse** und klicken Sie **Aktivieren**.
- In **Mozilla Firefox:**
  1. Öffnen Sie Mozilla Firefox.
  2. Klicken Sie auf Extras.
  3. Klicken Sie auf Add-ons.
  4. Klicken Sie auf Erweiterungen.
  5. Bewegen Sie den Mauszeiger auf **Bitdefender-Geldbörse** und klicken Sie **Aktivieren**.
- In **Google Chrome:**
  1. Öffnen Sie Google Chrome.
  2. Klicken Sie auf das Menü-Symbol.
  3. Klicken Sie auf Weitere Extras.
  4. Klicken Sie auf Erweiterungen.
  5. Bewegen Sie den Mauszeiger auf **Bitdefender-Geldbörse** und klicken Sie **Aktivieren**.

**Beachten Sie**
Das Add-on wird nach einem Neustart des Browsers aktiviert.

Überprüfen Sie jetzt, ob das automatische Einfügen für Ihre Online-Benutzerkonten funktioniert.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“ (S. 341)* beschrieben.

### 6.1.13. Entfernen von Bitdefender ist fehlgeschlagen

Wenn Sie Ihr Bitdefender-Produkt deinstallieren möchten und Sie bemerken, dass der Prozess hängen bleibt oder das System einfriert, klicken Sie auf **Abbrechen**. Sollte dies nicht zum Erfolg führen, starten Sie den Computer neu.

Falls die Deinstallation fehlschlägt, bleiben unter Umständen einige Bitdefender-Registry-Schlüssel und Dateien in Ihrem System. Solche Überbleibsel können eine erneute Installation von Bitdefender verhindern. Ebenso kann die Systemleistung und Stabilität leiden.

So können Sie Bitdefender vollständig von Ihrem System entfernen:

- In **Windows 7**:
  1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
  2. Suchen Sie **Bitdefender Total Security 2018** und wählen Sie **Deinstallieren**.
  3. Klicken Sie im angezeigten Fenster auf **Entfernen**.
  4. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.
- In **Windows 8 und Windows 8.1**:
  1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
  2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
  3. Suchen Sie **Bitdefender Total Security 2018** und wählen Sie **Deinstallieren**.
  4. Klicken Sie im angezeigten Fenster auf **Entfernen**.
  5. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.

- In **Windows 10**:
  1. Klicken Sie auf **Start** und danach auf Einstellungen.
  2. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie danach auf **Installierte Anwendungen**.
  3. Suchen Sie **Bitdefender Total Security 2018** und wählen Sie **Deinstallieren**.
  4. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.
  5. Klicken Sie im angezeigten Fenster auf **Entfernen**.
  6. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.

## 6.1.14. Mein System fährt nach der Installation von Bitdefender nicht mehr hoch

Wenn Sie Bitdefender gerade installiert haben und Ihr System nicht mehr im Normalmodus starten können, kann es verschiedene Ursachen für dieses Problem geben.

Höchstwahrscheinlich wird es durch eine vorherige Bitdefender-Installation hervorgerufen, die nicht vollständig entfernt wurde. Eine weitere Möglichkeit ist eine andere Sicherheitslösung, die noch auf dem System installiert ist.

Im Folgenden finden Sie Herangehensweisen für die verschiedenen Situationen:

- **Sie hatten Bitdefender schon einmal im Einsatz und danach nicht vollständig von Ihrem System entfernt.**

  So können Sie das Problem lösen:

  1. Starten Sie Ihren Computer im abgesicherten Modus neu. Eine Anleitung hierzu finden Sie im Kapitel *„Wie führe ich einen Neustart im abgesicherten Modus durch?“* (S. 89).
  2. Entfernen Sie Bitdefender von Ihrem System:
     - In **Windows 7**:
       a. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.

b. Suchen Sie **Bitdefender Total Security 2018** und wählen Sie **Deinstallieren**.

c. Klicken Sie im angezeigten Fenster auf **Entfernen**.

d. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.

e. Starten Sie Ihren Computer im Normalmodus neu.

- In **Windows 8 und Windows 8.1**:

  a. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.

  b. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.

  c. Suchen Sie **Bitdefender Total Security 2018** und wählen Sie **Deinstallieren**.

  d. Klicken Sie im angezeigten Fenster auf **Entfernen**.

  e. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.

  f. Starten Sie Ihren Computer im Normalmodus neu.

- In **Windows 10**:

  a. Klicken Sie auf **Start** und danach auf Einstellungen.

  b. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie danach auf **Installierte Anwendungen**.

  c. Suchen Sie **Bitdefender Total Security 2018** und wählen Sie **Deinstallieren**.

  d. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.

  e. Klicken Sie im angezeigten Fenster auf **Entfernen**.

  f. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.

  g. Starten Sie Ihren Computer im Normalmodus neu.

3. Installieren Sie Ihr Bitdefender-Produkt erneut.

- **Sie hatten zuvor eine andere Sicherheitslösung im Einsatz und haben diese nicht vollständig entfernt.**

  So können Sie das Problem lösen:

  1. Starten Sie Ihren Computer im abgesicherten Modus neu. Eine Anleitung hierzu finden Sie im Kapitel *„Wie führe ich einen Neustart im abgesicherten Modus durch?“* (S. 89).
  2. Entfernen Sie die andere Sicherheitslösung von Ihrem System:
     - In **Windows 7**:
       a. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
       b. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.
       c. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.
     - In **Windows 8 und Windows 8.1**:
       a. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
       b. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
       c. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.
       d. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.
     - In **Windows 10**:
       a. Klicken Sie auf **Start** und danach auf Einstellungen.
       b. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie danach auf **Installierte Anwendungen**.
       c. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.
       d. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.

Um die andere Software vollständig zu deinstallieren, rufen Sie die Hersteller-Website auf und führen Sie das entsprechende Deinstallations-Tool aus oder wenden Sie sich direkt an den Hersteller, um eine Deinstallationsanleitung zu erhalten.

3. Starten Sie Ihr System im Normalmodus neu und installieren Sie Bitdefender erneut.

**Sie haben die oben beschriebenen Schritte bereits durchgeführt und das Problem besteht weiterhin.**

So können Sie das Problem lösen:

1. Starten Sie Ihren Computer im abgesicherten Modus neu. Eine Anleitung hierzu finden Sie im Kapitel *„Wie führe ich einen Neustart im abgesicherten Modus durch?“* (S. 89).
2. Nutzen Sie die Systemwiederherstellung von Windows, um den Computer zu einem früheren Zeitpunkt wiederherzustellen, bevor das Bitdefender-Produkt installiert wurde.
3. Starten Sie das System im Normalmodus neu und wenden Sie sich an unsere Support-Mitarbeiter, wie in Abschnitt *„Hilfe anfordern“* (S. 341) beschrieben.

## 6.2. Entfernung von Bedrohungen

Bedrohungen können Ihr System auf vielfältige Art und Weise beeinträchtigen. Wie Bitdefender auf diese Malware darauf reagiert, hängt von der Art der Bedrohung ab. Da Bedrohungen ihr Verhalten ständig ändern, ist es schwierig ein Muster für ihr Verhalten und ihre Aktionen festzulegen.

Es gibt Situationen, in denen Bitdefender eine Bedrohung Ihres Systems nicht automatisch entfernen kann. In solch einem Fall ist Ihre Intervention nötig.

- *„Bitdefender-Rettungsmodus (Rettungsumgebung unter Windows 10)“* (S. 224)
- *„Wie gehe ich vor, wenn Bitdefender eine Bedrohung auf meinem Computer findet?“* (S. 228)
- *„Wie entferne ich eine Bedrohung aus einem Archiv?“* (S. 230)
- *„Wie entferne ich eine Bedrohung aus einem E-Mail-Archiv?“* (S. 231)
- *„Wie gehe ich vor, wenn ich eine Datei für gefährlich halte?“* (S. 232)

- *„Wobei handelt es sich bei den passwortgeschützten Dateien im Scan-Protokoll?“* (S. 232)
- *„Wobei handelt es sich bei den übersprungenen Objekten im Scan-Protokoll?“* (S. 233)
- *„Wobei handelt es sich bei den zu stark komprimierten Dateien im Scan-Protokoll?“* (S. 233)
- *„Warum hat Bitdefender ein infizierte Datei automatisch gelöscht?“* (S. 234)

Wenn Sie Ihr Problem hier nicht finden oder wenn die vorgeschlagene Lösung nicht zum Erfolg führt, können Sie den technischen Kundendienst von Bitdefender wie in Kapitel *„Hilfe anfordern“* (S. 341) beschrieben, kontaktieren.

## 6.2.1. Bitdefender-Rettungsmodus (Rettungsumgebung unter Windows 10)

Der **Rettungsmodus** ist eine Bitdefender-Funktion, mit der Sie alle bestehenden Festplattenpartitionen innerhalb und außerhalb Ihres Betriebssystems scannen und desinfizieren können.

Sobald Bitdefender Total Security 2018 unter **Windows 7, Windows 8 und Windows 8.1** installiert wurde und das Bitdefender-Rettungsmodus-Image heruntergeladen wurde, können Sie den Rettungsmodus verwenden, selbst wenn Sie Windows nicht mehr starten können.

Unter Windows 10 ist die Bitdefender-Rettungsumgebung in Windows RE integriert. Daher ist es bei diesem Betriebssystem nicht nötig, das Rettungsmodus-Image herunterzuladen. Die Funktion kann bei Systemstartproblemen nicht genutzt werden. Um das System vor dem Laden der Windows-Dienste zu bereinigen, empfehlen wir den Einsatz der Bitdefender-Rettungs-CD.

Bei der Bitdefender-Rettungs-CD handelt es sich um ein kostenloses Tool zur Bereinigung Ihres Computers bei Verdacht auf Beeinträchtigungen durch eine Bedrohung. Im Bitdefender-Support-Center unter http://www.bitdefender.de/support/consumer.html finden Sie nützliche Artikel mit weiteren Details zu ihrer Erstellung und Verwendung.

### Herunterladen des Bitdefender-Rettungsmodus-Images

Zur Verwendung des Rettungsmodus unter **Windows 7, Windows 8 und Windows 8.1** müssen Sie zunächst die Image-Datei wie folgt herunterladen:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Rettungsmodus**.
4. Klicken Sie im angezeigten Bestätigungsfenster auf **JA**, um Ihren Computer neu zu starten.

   Warten Sie, bis das Bitdefender-Rettungsmodus-Image von den Bitdefender-Servern heruntergeladen wurde. Sobald der Download abgeschlossen ist, wird der Computer neu gestartet.

   Ein Menü wird angezeigt, in dem Sie aufgefordert werden, ein Betriebssystem auszuwählen. Hier können Sie jetzt wählen, ob Sie Ihr System im Rettungs-Modus oder im normalen Modus starten möchten.

**Beachten Sie**
Aufgrund der Integration der Windows-Rettungsumgebung unter **Windows 10** ist der Download eines Rettungsmodus-Images bei diesem Betriebssystem nicht notwendig.

## Systemstart im Rettungsmodus unter Windows 7, Windows 8 und Windows 8.1

Es gibt zwei Möglichkeiten, den Rettungsmodus zu starten:

Über die Bitdefender-Benutzeroberfläche

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Rettungsmodus**.
4. Klicken Sie im angezeigten Bestätigungsfenster auf **JA**, um Ihren Computer neu zu starten.
5. Nach dem Neustart des Computers erscheint ein Menü, das Sie dazu auffordert, ein Betriebssystem auszuwählen. Wählen Sie **Bitdefender-Rettungsmodus** aus, um den Computer in einer Bitdefender-Umgebung zu starten, in der Sie Ihre Windows-Partition bereinigen können.

6. Wenn Sie dazu aufgefordert werden, drücken Sie die **Enter**-Taste und wählen Sie die Bildschirmauflösung, die am ehesten der von Ihnen sonst verwendeten Auflösung entspricht. Drücken Sie die **Eingabetaste** erneut.

   Der Bitdefender-Rettungsmodus wird innerhalb weniger Momente geladen.

Starten des Computers im Rettungsmodus

Wenn Windows nicht mehr startet, können Sie Ihren Computer direkt im Bitdefender-Rettungsmodus neu starten, indem Sie folgendermaßen vorgehen:

- In **Windows 7**:
  1. Drücken Sie **F8** bis der Bildschirm **Erweiterte Startoptionen** angezeigt wird.
  2. Wählen Sie den Bitdefender-Rettungsmodus über die Pfeiltasten aus und drücken Sie danach die **Eingabetaste**.

     Der Bitdefender-Rettungsmodus wird innerhalb weniger Momente geladen.
- In **Windows 8 und Windows 8.1**:
  1. Drücken Sie **Umschalttaste** bis der Bildschirm **Erweiterte Startoptionen** angezeigt wird.
  2. Wählen Sie die Option **Ein anderes Betriebssystem verwenden** und danach den Bitdefender-Rettungsmodus aus.

     Der Bitdefender-Rettungsmodus wird innerhalb weniger Momente geladen.

### Beachten Sie

Sie können Ihren Computer nur dann im Rettungsmodus starten, wenn Sie das Rettungsmodus-Image zuvor wie unter „Herunterladen des Bitdefender-Rettungsmodus-Images“ (S. 224) beschrieben heruntergeladen haben.

## Systemstart in der Rettungsumgebung unter Windows 10

Sie können den Rettungsmodus ausschließlich über Ihr Bitdefender-Produkt aufrufen. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
3. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Rettungsumgebung**.
4. Klicken Sie im angezeigten Fenster auf **Neustart**.

   Die Bitdefender-Rettungsumgebung wird innerhalb weniger Augenblicke geladen.

## Systemscans im Rettungsmodus (Rettungsumgebung unter Windows 10)

So scannen Sie Ihr System im Rettungsmodus (Rettungsumgebung):

- In **Windows 7, Windows 8 und Windows 8.1**:
  1. Starten Sie den Rettungsmodus, wie in Kapitel „Systemstart im Rettungsmodus unter Windows 7, Windows 8 und Windows 8.1“ (S. 225) beschrieben.
  2. Das Bitdefender-Logo wird angezeigt und der Kopiervorgang für die Engines der Sicherheitslösung beginnt.
  3. Ein Willkommensfenster wird angezeigt. Klicken Sie auf **Fortfahren**.
  4. Ein Update der Bedrohungsinformationsdatenbank wird gestartet.
  5. Nach Abschluss des Updates wird das Fenster für den Bitdefender-Bedarf-Scan angezeigt.
  6. Klicken Sie auf **Jetzt scannen**, wählen Sie in dem jetzt erscheinenden Fenster das Scan-Ziel aus und klicken Sie auf **Öffnen**, um den Scan zu starten.

     Wir empfehlen Ihnen, Ihre gesamte Windows-Partition zu scannen.

     > **Beachten Sie**
     > Wenn Sie den Rettungsmodus nutzen, werden Ihnen die Namen der Partitionen im Linux-Format angezeigt. Die Festplattenpartitionen werden angezeigt als sda1, was wahrscheinlich der Windows-Partition (C:) entspricht, sda2, was (D:) entspricht usw.

  7. Warten Sie, bis der Scan abgeschlossen ist. Befolgen Sie die Anweisungen, um gefundene Bedrohungen zu entfernen.

8. Um den Rettungsmodus zu beenden, klicken Sie mit der rechten Maustaste auf einen leeren Bereich auf dem Desktop, klicken Sie im Kontextmenü auf **Verlassen** und wählen Sie dann, ob Sie den Computer neu starten oder herunterfahren möchten.

- In **Windows 10**:

1. Starten Sie die Rettungsumgebung, wie beschrieben in „Systemstart in der Rettungsumgebung unter Windows 10“ (S. 226).
2. Der Bitdefender-Scan-Prozess wird automatisch gestartet, sobald das System in der Rettungsumgebung geladen wird.
3. Warten Sie, bis der Scan abgeschlossen ist. Befolgen Sie die Anweisungen, um gefundene Bedrohungen zu entfernen.
4. Klicken Sie zum Beenden der Rettungsumgebung im Fenster mit den Scan-Ergebnissen auf **SCHLIEßEN**.

## 6.2.2. Wie gehe ich vor, wenn Bitdefender eine Bedrohung auf meinem Computer findet?

Sie erfahren unter Umständen auf eine der folgenden Arten, dass auf Ihrem Computer eine Bedrohung vorliegt:

- Sie haben einen Scan durchgeführt und Bitdefender hat infizierte Einträge gefunden.
- Eine Bedrohungswarnung informiert Sie, dass Bitdefender einen oder mehrere Bedrohungen auf Ihrem Computer geblockt hat.

In solchen Situationen sollten Sie Bitdefender aktualisieren, um sicherzustellen, dass Sie über die neuesten Bedrohungsinformationen verfügen und einen System-Scan durchführen, um das System zu prüfen.

Sobald der System-Scan abgeschlossen ist, wählen Sie die gewünschte Aktion für die infizierten Objekte aus (Desinfizieren, Löschen, In Quarantäne verschieben).

### Warnung

Wenn Sie den Verdacht haben, dass die Datei Teil des Windows-Betriebssystems ist oder dass es sich nicht um eine infizierte Datei handelt, folgen Sie NICHT diesen Schritten und kontaktieren Sie so bald wie möglich den Bitdefender-Kundendienst.

Falls die ausgewählte Aktion nicht durchgeführt werden konnte und im Scan-Protokoll ersichtlich ist, dass Ihr PC mit einer Bedrohung infiziert ist, die nicht gelöscht werden kann, müssen Sie die Datei(en) manuell entfernen.

**Die erste Methode kann im Normalmodus eingesetzt werden**:

1. Deaktivieren Sie den Bitdefender-Echtzeitvirenschutz:
   a. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
   b. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
   c. Klicken Sie auf das -Symbol unten rechts im Bereich **VIRENSCHUTZ**.
   d. Klicken Sie im Fenster **SCHILD** auf den AN/AUS-Schalter.
2. Lassen Sie sich die verborgenen Objekte in Windows anzeigen. Eine Anleitung hierzu finden Sie im Kapitel *„Wie kann ich in Windows versteckte Objekte anzeigen?“* (S. 87).
3. Blättern Sie zum Laufwerk, in dem die infizierte Datei gespeichert ist (siehe Scan-Protokoll) und löschen Sie sie.
4. Aktivieren Sie den Bitdefender-Echtzeitvirenschutz.

**Falls die Infektion mit der ersten Methode nicht entfernt werden konnte**:

1. Starten Sie Ihren Computer im abgesicherten Modus neu. Eine Anleitung hierzu finden Sie im Kapitel *„Wie führe ich einen Neustart im abgesicherten Modus durch?“* (S. 89).
2. Lassen Sie sich die verborgenen Objekte in Windows anzeigen. Eine Anleitung hierzu finden Sie im Kapitel *„Wie kann ich in Windows versteckte Objekte anzeigen?“* (S. 87).
3. Blättern Sie zum Laufwerk, in dem die infizierte Datei gespeichert ist (siehe Scan-Protokoll) und löschen Sie sie.
4. Starten Sie Ihren Computer neu und starten Sie den Normalmodus.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“* (S. 341) beschrieben.

## 6.2.3. Wie entferne ich eine Bedrohung aus einem Archiv?

Bei einem Archiv handelt es sich um eine Datei oder eine Dateisammlung, die mit einem speziellen Format komprimiert wurde, um so den benötigten Festplattenplatz zu reduzieren.

Einige dieser Formate sind offene Formate und bieten Bitdefender die Möglichkeit, diese zu scannen und die entsprechenden Aktionen durchzuführen, um sie zu entfernen.

Andere Archivformate sind teilweise oder komplett geschlossen und Bitdefender kann nur das Vorhandensein von Bedrohungen innerhalb dieser Archive feststellen, nicht jedoch andere Aktionen ausführen.

Wenn Bitdefender Sie darüber informiert, dass eine Bedrohung innerhalb eines Archivs gefunden wurde und keine Aktion verfügbar ist, bedeutet dies, dass die Bedrohung aufgrund möglicher Restriktionen der Zugriffseinstellungen des Archivs nicht entfernt werden kann.

So können Sie eine in einem Archiv gespeicherte Bedrohung entfernen.

1. Führen Sie einen System-Scan durch, um das Archiv zu finden, in dem sich die Bedrohung befindet.
2. Deaktivieren Sie den Bitdefender-Echtzeitvirenschutz:
   a. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
   b. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
   c. Klicken Sie auf das -Symbol unten rechts im Bereich **VIRENSCHUTZ**.
   d. Klicken Sie im Fenster **SCHILD** auf den AN/AUS-Schalter.
3. Gehen Sie zum Speicherort des Archivs und dekomprimieren Sie es mit einem Archivierungsprogramm wie beispielsweise WinZip.
4. Identifizieren Sie die infizierte Datei und löschen Sie sie.
5. Löschen Sie das Originalarchiv, um sicherzugehen, dass die Infizierung vollständig entfernt ist.
6. Komprimieren Sie die Dateien erneut in einem neuen Verzeichnis und verwenden Sie dafür ein Komprimierprogramm wie WinZip.

7. Aktivieren Sie den Bitdefender-Echtzeit-Virenschutz und führen Sie einen System-Scan durch, um so sicherzustellen, dass Ihr System nicht anderweitig infiziert ist.

> **Beachten Sie**
> Es ist wichtig zu beachten, dass eine in einem Archiv gespeicherte Bedrohung für Ihr System keine unmittelbare Bedrohung darstellt, da die Bedrohung dekomprimiert und ausgeführt werden muss, bevor sie Ihr System infizieren kann.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“ (S. 341)* beschrieben.

## 6.2.4. Wie entferne ich eine Bedrohung aus einem E-Mail-Archiv?

Bitdefender kann auch Bedrohungen in E-Mail-Datenbanken und auf Festplatten gespeicherten E-Mail-Archiven aufspüren.

Manchmal ist es notwendig, die infizierte Nachricht über die im Scan-Bericht zur Verfügung gestellten Informationen zu identifizieren und sie dann manuell zu löschen.

So können Sie in einem E-Mail-Archiv gespeicherte Bedrohungen entfernen:

1. Scannen Sie die E-Mail-Datenbank mit Bitdefender.
2. Deaktivieren Sie den Bitdefender-Echtzeitvirenschutz:
   a. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
   b. Klicken Sie auf **FUNKTIONEN ANZEIGEN**.
   c. Klicken Sie auf das -Symbol unten rechts im Bereich **VIRENSCHUTZ**.
   d. Klicken Sie im Fenster **SCHILD** auf den AN/AUS-Schalter.
3. Öffnen Sie den Scan-Bericht und nutzen Sie die Identifikationsinformation (Betreff, Von, An) der infizierten Nachricht, um den dazugehörigen E-Mail-Client zu finden.
4. Löschen Sie die infizierte Nachricht. Die meisten E-Mail-Clients verschieben gelöschte Nachrichten in ein Wiederherstellungsordner, von dem aus sie

wiederhergestellt werden können. Sie sollten sicherstellen, dass die Nachricht auch aus diesem Recovery-Verzeichnis gelöscht ist.

5. Komprimieren Sie das Verzeichnis, in dem die infizierte Nachricht gespeichert wird.
   - In Microsoft Outlook 2007: Klicken Sie im Dateimenü auf "Datendateiverwaltung". Wählen Sie das persönliche Verzeichnis (.pst), das Sie komprimieren möchten und klicken Sie auf "Einstellungen". Klicken Sie auf Jetzt komprimieren.
   - In Microsoft Outlook 2010 / 2013/ 2016: Klicken Sie im Dateimenü auf Info und dann Kontoeinstellungen (Konten hinzufügen oder entfernen bzw. vorhandene Verbindungseinstellungen ändern). Klicken Sie danach auf Datendatei, markieren Sie die persönlichen Ordner-Dateien (.pst), die Sie komprimieren wollen, und klicken Sie auf Einstellungen. Klicken Sie auf Jetzt komprimieren.
6. Aktivieren Sie den Bitdefender-Echtzeitvirenschutz.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“ (S. 341)* beschrieben.

## 6.2.5. Wie gehe ich vor, wenn ich eine Datei für gefährlich halte?

Möglicherweise halten Sie eine Datei auf Ihrem System für gefährlich, obwohl Ihr Bitdefender-Produkt keine Gefahr erkannt hat.

So können Sie sicherstellen, dass Ihr System geschützt ist:

1. Führen Sie einen **System-Scan** mit Bitdefender durch. Eine Anleitung hierzu finden Sie im Kapitel *„Wie scanne ich mein System?“ (S. 63)*.
2. Wenn der Scan ein sauberes Ergebnis liefert, Sie aber weiterhin Zweifel an der Sicherheit der Datei hegen und ganz sicher gehen möchten, wenden Sie sich bitte an unsere Support-Mitarbeiter, damit wir Ihnen helfen können.

   Eine Anleitung hierzu finden Sie im Kapitel *„Hilfe anfordern“ (S. 341)*.

## 6.2.6. Wobei handelt es sich bei den passwortgeschützten Dateien im Scan-Protokoll?

Dies ist nur eine Benachrichtigung, dass die von Bitdefender gefundenen Dateien entweder passwortgeschützt oder anderweitig verschlüsselt sind.

Am häufigsten sind passwortgeschützte Objekte:

- Dateien, die zu einer anderen Sicherheitslösung gehören.
- Dateien, die zum Betriebssystem gehören.

Um die Inhalte tatsächlich zu scannen, müssen diese Dateien entweder extrahiert oder anderweitig entschlüsselt werden.

Sollten diese Inhalte extrahiert werden, wird der Echtzeit-Scanner von Bitdefender diese automatisch scannen, um so den Schutz Ihres Computers zu gewährleisten. Wenn Sie diese Dateien mit Bitdefender scannen möchten, müssen Sie den Produkthersteller kontaktieren, um nähere Details zu diesen Dateien zu erhalten.

Unsere Empfehlung ist, diese Dateien zu ignorieren, da Sie für Ihr System keine Bedrohung darstellen.

## 6.2.7. Wobei handelt es sich bei den übersprungenen Objekten im Scan-Protokoll?

Alle Dateien, die im Scan-Protokoll als "Übersprungen" ausgewiesen werden, sind sauber.

Für eine bessere Leistung scannt Bitdefender keine Dateien, die seit dem letzten Scan nicht verändert wurden.

## 6.2.8. Wobei handelt es sich bei den zu stark komprimierten Dateien im Scan-Protokoll?

Die zu stark komprimierten Objekte sind Elemente, die durch die Scan-Engine nicht extrahiert werden konnten oder Elemente, für die eine Entschlüsselung zu viel Zeit in Anspruch genommen hätte und die dadurch das System instabil machen würden.

Überkomprimiert bedeutet, dass Bitdefender das Scannen von Archiven übersprungen hat, da das Entpacken dieser zu viele Systemressourcen in Anspruch genommen hätte. Der Inhalt wird, wenn nötig, in Echtzeit gescannt.

## 6.2.9. Warum hat Bitdefender ein infizierte Datei automatisch gelöscht?

Wird eine infizierte Datei gefunden, versucht Bitdefender automatisch, diese zu desinfizieren. Falls die Desinfizierung fehlschlägt, wird die Datei in die Quarantäne verschoben, um dort die Infizierung einzudämmen.

Bestimmte Bedrohungsarten können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

Dies geschieht normalerweise bei Installationsdateien, die von nicht vertrauenswürdigen Seiten heruntergeladen werden. Wenn Sie auf ein solches Problem stoßen, laden Sie die Installationsdatei von der Website des Herstellers oder einer anderen vertrauenswürdigen Website herunter.

# ANTIVIRUS FÜR MAC

# 7. INSTALLATION UND DEINSTALLATION

Dieses Kapital beinhaltet die folgenden Themen:

- *„Systemanforderungen“* (S. 236)
- *„Installation von Bitdefender Antivirus for Mac“* (S. 236)
- *„Bitdefender Antivirus for Mac entfernen“* (S. 241)

## 7.1. Systemanforderungen

Sie können Bitdefender Antivirus for Mac nur auf Intel-basierten Macintosh Computern mit OS X Mavericks(10.9.5), OS X Yosemite (ab 10.10.5), OS X El Capitan (10.11.6), macOS Sierra (ab 10.12.5), macOS High Sierra 10.13 installieren.

Ihr Mac muss zudem auch alle folgenden Anforderungen erfüllen:

- Minimum 1 GB Arbeitsspeicher
- Minimum 600 MB freier Speicherplatz auf der Festplatte

Für die Registrierung und Updates von Bitdefender Antivirus for Mac ist eine aktive Internetverbindung notwendig.

### So finden Sie heraus, welche macOS-Version und Hardware Sie nutzen

Klicken Sie in der linken oberen Bildschirmecke auf das Apple-Symbol und wählen Sie **Über diesen Mac**. Im sich öffnenden Fenster werden Ihre Betriebssystem-Version und andere nützliche Informationen eingeblendet. Klicken Sie auf **Mehr Infos**, um detaillierte Informationen zur Hardware zu erhalten.

## 7.2. Installation von Bitdefender Antivirus for Mac

Die Bitdefender Antivirus for Mac-App kann wie folgt über Ihr Bitdefender-Benutzerkonto installiert werden:

1. Als Administrator anmelden.
2. Gehen Sie zu: https://central.bitdefender.com.
3. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Bitdefender-Konto an.

4. Rufen Sie den Bereich **Meine Geräte** auf und klicken Sie auf **LOKALEN SCHUTZ INSTALLIEREN**.
5. Wählen Sie eine der beiden verfügbaren Optionen:
   - **HERUNTERLADEN**

     Klicken Sie auf die Schaltfläche und speichern Sie die Installationsdatei.
   - **Auf einem anderen Gerät**

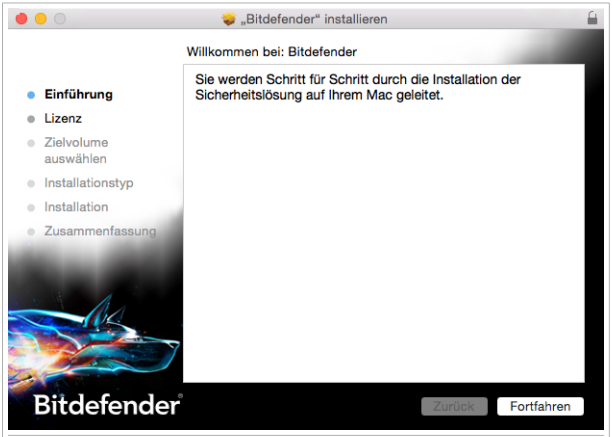
     Wählen Sie **macOS** aus, um Ihr Bitdefender-Produkt herunterzuladen und klicken Sie danach auf **FORTFAHREN**. Geben Sie Ihre E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **SENDEN**.
6. Führen Sie das von Ihnen heruntergeladene Bitdefender aus.
7. Führen Sie die Installationsschritte durch.

### 7.2.1. Installationsvorgang

Anleitung zur Installation von Bitdefender Antivirus for Mac:

1. Klicken Sie auf die heruntergeladene Datei. Der Installationsassistent wird geöffnet und führt Sie durch den Installationsvorgang.
2. Folgen Sie den Anweisungen des Installationsassistenten.

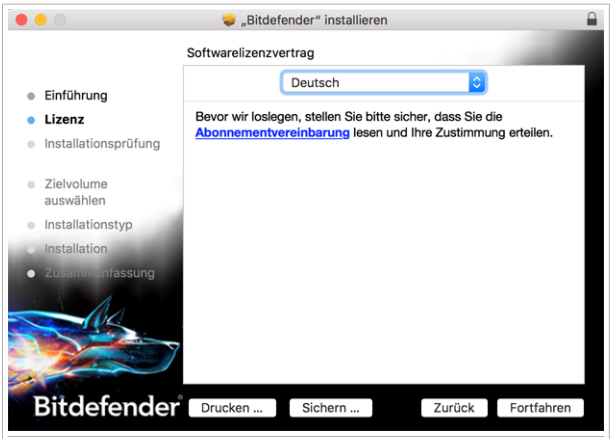
## Schritt 1 - Willkommensfenster




Begrüßungsfenster

Klicken Sie auf **Fortfahren**.

## Schritt 2 - Lesen Sie die Abonnementvereinbarung




Lesen Sie die Abonnementvereinbarung

Bevor Sie mit der Installation fortfahren, müssen Sie zunächst der Abonnementvereinbarung zustimmen. Bitte nehmen Sie sich einen Moment

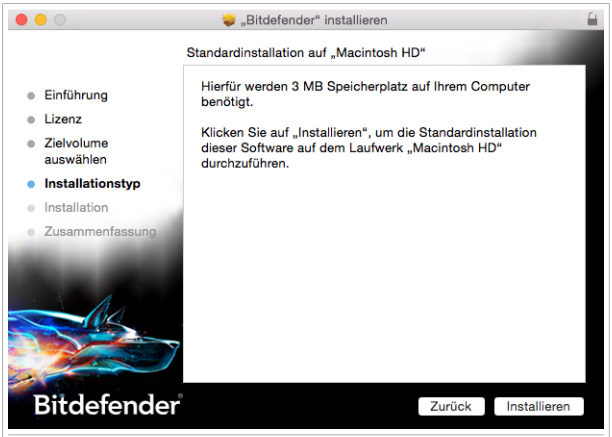
Zeit, um die Abonnementvereinbarung zu lesen, da Sie hier die Bedingungen finden, unter denen Sie Bitdefender Antivirus for Mac nutzen dürfen.

Klicken Sie auf **Weiter** und danach auf **Zustimmen**.

**Wichtig**

Falls Sie die Nutzungsbedingungen nicht akzeptieren möchten, klicken Sie auf **Weiter** und dann auf **Nicht zustimmen**. Der Installationsvorgang wird dann abgebrochen und der Installationsassistent geschlossen.

## Schritt 3 - Installation starten

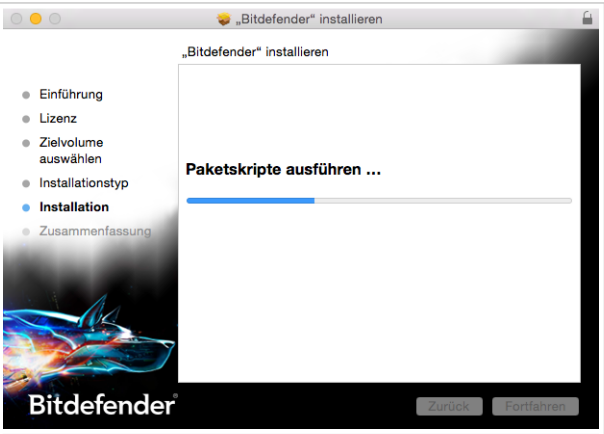



Installation starten

Bitdefender Antivirus for Mac wird installiert in Macintosh HD/Library/Bitdefender. Der Installationspfad kann nicht geändert werden.

Klicken Sie auf **Installieren**, um die Installation zu starten.

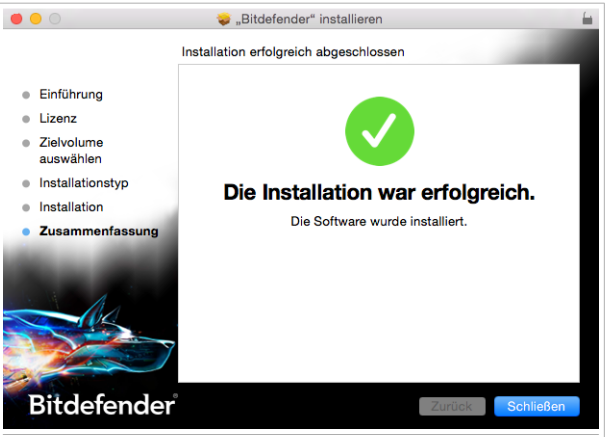
## Schritt 4 - Installiert Bitdefender Antivirus for Mac




Installation von Bitdefender Antivirus for Mac

Warten Sie, bis die Installation abgeschlossen ist und klicken Sie auf **Weiter**.

## Schritt 5 - Fertigstellung




Fertigstellen

Klicken Sie auf **Schließen**, um das Installationsfenster zu schließen.

Damit ist der Installationsvorgang abgeschlossen.

**Wichtig**
Wenn Sie Bitdefender Antivirus for Mac unter macOS High Sierra 10.13 oder einer neueren Version installieren, wird die Meldung **System-Erweiterung blockiert** angezeigt. Sie weist Sie darauf hin, dass die von Bitdefender signierten Erweiterungen blockiert wurden und manuell aktiviert werden müssen. Klicken Sie auf **Weiter**. Klicken Sie im daraufhin angezeigten Bitdefender Antivirus for Mac-Fenster auf den Link **Sicherheit & Privatsphäre**. Markieren Sie das Kästchen Bitdefender in der Liste und klicken Sie auf **OK**.

Bei der ersten Installation von Bitdefender Antivirus for Mac werden die Assistenten für Safe Files und den Time-Machine-Schutz angezeigt. Weitere Informationen finden Sie in den Abschnitten *„Sichere Dateien“ (S. 260)* und *„Time-Machine-Schutz“ (S. 248)*.

Sie erhalten eine Einführung in die VPN-Funktion. Klicken Sie auf **Weiter**. Weitere Informationen finden Sie unter *„VPN“ (S. 286)*.

## 7.3. Bitdefender Antivirus for Mac entfernen

Bitdefender Antivirus for Mac ist eine komplexe Anwendung und kann nicht auf herkömmliche Weise deinstalliert werden, indem das Symbol für die Anwendung aus dem Verzeichnis Anwendungen in den Papierkorb gezogen wird.

Um Bitdefender Antivirus for Mac zu entfernen, gehen Sie folgendermaßen vor:

1. Öffnen Sie **Finder** und wählen Sie den Programme-Ordner.
2. Öffnen Sie den Bitdefender-Ordner und doppelklicken Sie nach auf Bitdefender-Deinstallationsprogramm.
3. Klicken Sie auf **Deinstallieren**, und warten Sie, bis der Vorgang abgeschlossen ist.
4. Klicken Sie zum Abschluss auf **Schließen**.

**Wichtig**
Ist ein Fehler aufgetreten, so können Sie die Kundenbetreuung von Bitdefender wie in *„Hilfe anfordern“ (S. 341)* beschrieben, kontaktieren.

# 8. ERSTE SCHRITTE

Dieses Kapital beinhaltet die folgenden Themen:

- *„Über Bitdefender Antivirus for Mac“* (S. 242)
- *„Öffnen Sie Bitdefender Antivirus for Mac“* (S. 242)
- *„Das Hauptfenster“* (S. 243)
- *„Dock-Symbol der App“* (S. 244)

## 8.1. Über Bitdefender Antivirus for Mac

Bitdefender Antivirus for Mac ist ein leistungsstarker Virenscanner, der alle Arten von Schad-Software („Bedrohungen“) erkennen und entfernen kann:

- Ransomware
- Adware
- Viren
- Spyware
- Trojaner
- Keylogger
- Computerwürmer

Diese App erkennt und entfernt nicht nur Mac-spezifische, sondern auch Windows-spezifische Bedrohungen und verhindert so, dass Sie infizierte Dateien versehentlich an die PCs Ihrer Familie, Freunde und Kollegen weiterleiten.

## 8.2. Öffnen Sie Bitdefender Antivirus for Mac

Sie haben mehrere Möglichkeiten Bitdefender Antivirus for Mac zu öffnen.

- Klicken Sie im Launchpad auf das "Bitdefender Antivirus for Mac"-Symbol.
- Klicken Sie in der Menüleiste auf das Symbol und wählen Sie **Hauptfenster öffnen**.
- Öffnen Sie ein Finder-Fenster, wählen Sie Anwendungen aus und doppelklicken Sie auf das Bitdefender Antivirus for Mac-Symbol.

## 8.3. Das Hauptfenster

Im Hauptfenster der Anwendung wird der Sicherheitsstatus Ihres Computers angezeigt. Dort können Sie auch System-Scans starten, das Surfen im Internet sicherer machen und sich bei Ihrem Bitdefender-Konto anmelden.

Das Hauptfenster

Die Funktion **Autopilot** befindet sich in der rechten oberen Ecke des Hauptfensters. Sie überwacht durchgehend sämtliche auf dem Computer laufenden Anwendungen, sucht nach Aktionen, die auf Bedrohungen hinweisen könnten, und verhindert so, dass neue Bedrohungen auf das System gelangt.

Aus Sicherheitsgründen wird empfohlen, den Autopiloten nicht zu deaktivieren. Wenn er deaktiviert wird, sind Sie nicht automatisch vor Bedrohungen geschützt.

Die Statusleiste oben im Fenster informiert Sie mit eindeutigen Meldungen und Farbanzeigen über den Sicherheitsstatus des Systems. Liegen keine Warnungen in Bitdefender Antivirus for Mac vor, ist die Statusleiste grün. Wenn ein Sicherheitsproblem gefunden wurde, ändert die Statusleiste ihre Farbe auf gelb. Mit einem Klick auf die Schaltfläche **Probleme anzeigen** können Sie die Probleme anzeigen, die die Sicherheit Ihres Systems

gefährden. Detaillierte Informationen zu Problemen und wie diese beseitigt werden können, finden Sie unter *„Alle beheben“ (S. 251)*.

Unterhalb der Statusleiste finden Sie drei Scan-Schaltflächen, mit denen Sie Ihren Mac scannen lassen können:

- **Quick Scan** - überprüft die sensibelsten Verzeichnisse Ihres Systems (beispielsweise die Verzeichnisse mit Dokumenten, Downloads, Mail-Downloads und temporären Dateien eines Benutzers) auf Bedrohungen.
- **Vollständiger Scan** - überprüft das gesamte System umfassend auf Bedrohungen. Alle eingebundenen Dateisysteme werden ebenfalls gescannt.
- **Benutzerdefinierter Scan** - hiermit können einzelne Dateien, Verzeichnisse etc. auf Bedrohungen geprüft werden.

Weitere Informationen finden Sie unter *„Ihren Mac scannen“ (S. 247)*.

Neben den Scan-Schaltflächen sind noch weitere Optionen verfügbar:

- **Internet-Schutz** - Filtert den Internet-Verkehr und blockiert alle schädlichen Inhalte, um Ihnen sicheres Surfen zu ermöglichen. Weitere Informationen finden Sie unter *„Internet-Schutz“ (S. 252)*.
- **Bitdefender-Konto aufrufen** - Klicken Sie auf den Link **Zum eigenen Konto** links unten in der Benutzeroberfläche, um Ihren Bitdefender-Konto aufzurufen. Weitere Informationen finden Sie unter *„Bitdefender Central“ (S. 270)*.
- **Verbleibende Tage** - hier wird die verbleibende Zeit bis zum Ablauf Ihres Abonnements angezeigt. Wurde das Ablaufdatum erreicht, klicken Sie auf den Link, um eine Website aufzurufen, auf der Sie Ihr Abonnement verlängern können.
- **Kaufen** - Öffnet die Bitdefender-Website, auf der Sie alle Angebote durchstöbern oder direkt ein Abonnement erwerben können.
- **Feedback** - Öffnet ein neues Fenster in Ihrem E-Mail-Programm, über das Sie uns kontaktieren können.

## 8.4. Dock-Symbol der App

Das "Bitdefender Antivirus for Mac"-Symbol wird sofort nach Öffnen der Anwendung im Dock angezeigt. Über das Symbol im Dock können Sie Dateien

und Order schnell und einfach auf Bedrohungen prüfen. Ziehen Sie die Datei oder den Ordner einfach per Drag und Drop auf das Symbol im Dock, um den Scan sofort zu starten.

Produktsymbol im Dock

# 9. SCHUTZ GEGEN BÖSARTIGE SOFTWARE

Dieses Kapital beinhaltet die folgenden Themen:


- *„Empfohlene Vorgehensweisen“* (S. 246)
- *„Ihren Mac scannen“* (S. 247)
- *„Den Autopiloten ein- und ausschalten“* (S. 248)
- *„Time-Machine-Schutz“* (S. 248)
- *„Scan-Assistent“* (S. 250)
- *„Alle beheben“* (S. 251)
- *„Internet-Schutz“* (S. 252)
- *„Updates“* (S. 254)


## 9.1. Empfohlene Vorgehensweisen

Um Ihr System vor Bedrohungen zu schützen und eine versehentliche Infizierung anderer Systeme zu verhindern, sollten Sie folgende Empfehlungen beachten:

- Der **Autopilot** sollte immer aktiviert sein, damit Bitdefender Antivirus for Mac Ihre Systemdateien scannen kann.
- Sie sollten Bitdefender Antivirus for Mac über Produkt-Updates immer auf dem neuesten Stand halten. Zudem sollte der **Autopilot** stets aktiviert bleiben.
- Überprüfen und beheben Sie die von Bitdefender Antivirus for Mac aufgelistetenProbleme regelmäßig. Detaillierte Informationen finden Sie unter *„Alle beheben“* (S. 251).
- Überprüfen Sie das detaillierte Ereignisprotokoll mit allen Bitdefender Antivirus for Mac-Aktivitäten auf Ihrem Computer. Für jedes sicherheitsrelevante Ereignis, das Ihr System oder Ihre Daten betrifft, wird dem Bitdefender-Verlauf eine neue Nachricht hinzugefügt. Weitere Details dazu finden Sie hier: *„Verlauf“* (S. 263).
- Darüber hinaus sollten Sie folgende Empfehlungen berücksichtigen:

- Sie sollten grundsätzlich alle Dateien scannen, die Sie von externen Speichern (z.B. USB-Sticks oder CDs) herunterladen, insbesondere wenn Ihnen die Quelle nicht bekannt ist.
- Bei DMG-Dateien sollten diese zunächst gemountet und dann ihr Inhalt (die Dateien im gemounteten Volume/Image) gescannt werden.

Der einfachste Weg, eine Datei, Verzeichnis etc. zu scannen ist, diese per drag&drop in das Anwendungsfenster von Bitdefender Antivirus for Mac oder das Dock-Symbol zu ziehen.

Es sind keine weitere Konfigurationen oder Aktionen erforderlich. Sie können jedoch bei Bedarf Anpassungen an den Einstellungen vornehmen. Weitere Informationen finden Sie unter *„Einstellungen konfigurieren“* (S. 257).

## 9.2. Ihren Mac scannen

Außer dem **Autopiloten**, der fortlaufend alle Anwendungen überwacht, die auf Ihrem Computer laufen, und dabei nach Aktionen sucht, die auf Bedrohungen hindeuten, und außerdem verhindert, dass neue Bedrohungen auf Ihr System gelangen, können Sie das System oder einzelne Dateien jederzeit nach Bedarf scannen.

Der einfachste Weg, eine Datei, Verzeichnis etc. zu scannen ist, diese per drag&drop in das Anwendungsfenster von Bitdefender Antivirus for Mac oder das Dock-Symbol zu ziehen. Der Scan-Assistent wird angezeigt. Er führt Sie durch den Scan-Vorgang.

Sie können einen Scan wie folgt starten:

1. Öffnen Sie Bitdefender Antivirus for Mac.
2. Klicken Sie auf einen der drei Scan-Schaltflächen, um den gewünschten Scan zu starten.
   - **Quick Scan** - überprüft die sensibelsten Verzeichnisse Ihres Systems (beispielsweise die Verzeichnisse mit Dokumenten, Downloads, Mail-Downloads und temporären Dateien eines Benutzers) auf Bedrohungen.
   - **Vollständiger Scan** - überprüft das gesamte System umfassend auf Bedrohungen. Alle eingebundenen Dateisysteme werden ebenfalls gescannt.

### Beachten Sie

Je nach Größe Ihrer Festplatte kann ein vollständiger System-Scan einige Zeit in Anspruch nehmen (bis zu einer Stunde und mehr). Um die Systemleistung nicht zu beeinträchtigen, sollte diese Aufgabe nicht zeitgleich mit anderen ressourcenintensiven (z.B. Videobearbeitung) Aufgaben ausgeführt werden.
Falls gewünscht, können Sie bestimmte Laufwerke vom Scan ausschließen, indem Sie sie in den Einstellungen zur Liste der Ausschlüsse hinzufügen.

- **Benutzerdefinierter Scan** - hiermit können einzelne Dateien, Verzeichnisse etc. auf Bedrohungen geprüft werden.

## 9.3. Den Autopiloten ein- und ausschalten

Wählen Sie eine der folgenden Methoden, um den Autopiloten ein- oder auszuschalten:

- Öffnen Sie Bitdefender Antivirus for Mac und klicken Sie auf den Schalter, um den Autopiloten ein- oder auszuschalten.
- Klicken Sie in der Menüleiste auf das Symbol und wählen Sie **Autopilot ausschalten**.

### Warnung

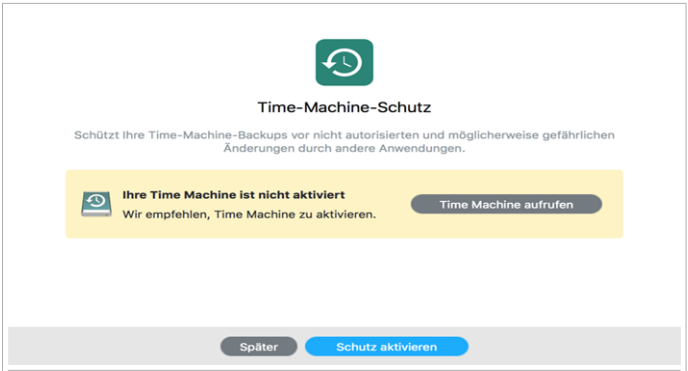
Wir empfehlen, den Autopiloten nur für möglichst kurze Zeit zu deaktivieren. Wenn er deaktiviert wird, sind Sie nicht automatisch vor Bedrohungen geschützt.

## 9.4. Time-Machine-Schutz

Der Bitdefender-Time-Machine-Schutz bietet zusätzliche Sicherheit für Ihr Backup-Laufwerk und alle darauf gespeicherten Dateien, indem es den Zugriff durch externe Quellen verhindert. Werden Dateien in Ihrem Time-Machine-Laufwerk von Ransomware verschlüsselt, können Sie sie auch ohne Lösegeldzahlung wiederherstellen.

### Assistent für den Time-Machine-Schutz

Der Assistent für den Bitdefender-Time-Machine-Schutz wird bei der ersten Installation von Bitdefender Antivirus for Mac auf Ihrem Macintosh angezeigt.




Assistent für den Time-Machine-Schutz

Sie müssen die Time-Machine-Datensicherung einrichten, bevor Sie den Bitdefender-Schutz aktivieren.

Gehen Sie folgendermaßen vor, falls die Time-Machine-Funktion auf Ihrem System noch nicht aktiviert ist:

1. Klicken Sie auf die Option **Time Machine aufrufen**.

   Das **Time Machine**-Fenster aus den Systemeinstellungen wird geöffnet.

2. Aktivieren Sie die Funktion und legen Sie fest, wo Ihre Sicherungsdateien aufbewahrt werden sollen.

Falls Sie weitere Informationen zur Aktivierung der Time-Machine-Anwendung auf Ihrem System benötigen, klicken Sie im Assistenten auf **Lernen Sie, wie man Time Machine konfiguriert.**.

So aktivieren Sie den Bitdefender-Time-Machine-Schutz für Ihre Sicherungskopien:

1. Aktivieren Sie die Option **Schutz aktivieren**.

   Ein Bestätigungsfenster wird angezeigt.

2. Klicken Sie auf **Schließen**.

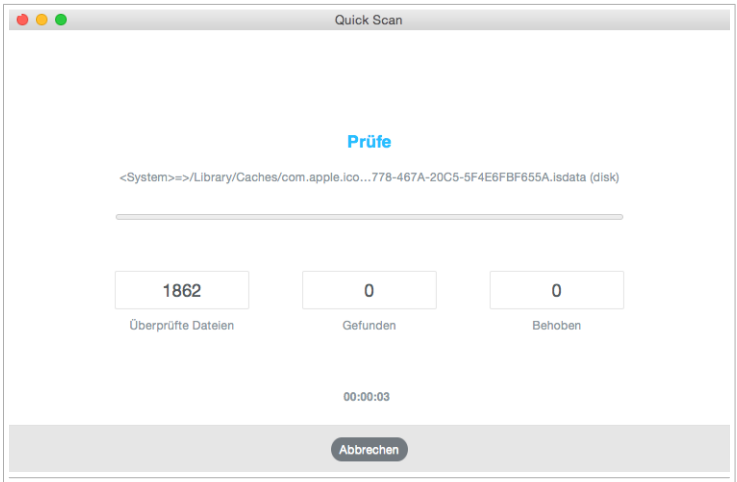
## Aktivierung und Deaktivierung des Time-Machine-Schutzes

So können Sie den Time-Machine-Schutz aktivieren oder deaktivieren:

1. Öffnen Sie Bitdefender Antivirus for Mac.
2. Klicken Sie in der Menüleiste auf Bitdefender Antivirus for Mac und wählen Sie **Präferenzen**.
3. Wechseln Sie zum Reiter **Schutz**.
4. Aktivieren oder deaktivieren die das Kästchen **Time-Machine-Schutz**.

## 9.5. Scan-Assistent

Sobald Sie einen Scan starten, öffnet sich der Bitdefender Antivirus for Mac-Assistent.




Scan läuft...

Während eines Scans werden Informationen zu gefundenen und behobenen Bedrohungen in Echtzeit angezeigt.

Bitte warten Sie, bis Bitdefender Antivirus for Mac den Scan beendet hat.

**Beachten Sie**
Der Scan-Vorgang kann, abhängig von der Größe Ihrer Festplatte, eine Weile dauern.

## 9.6. Alle beheben

Bitdefender Antivirus for Mac spürt automatisch mögliche Probleme, die die Sicherheit Ihres Systems beeinflussen können, auf und informiert Sie. So können Sicherheitsrisiken einfach und frühzeitig behoben werden.

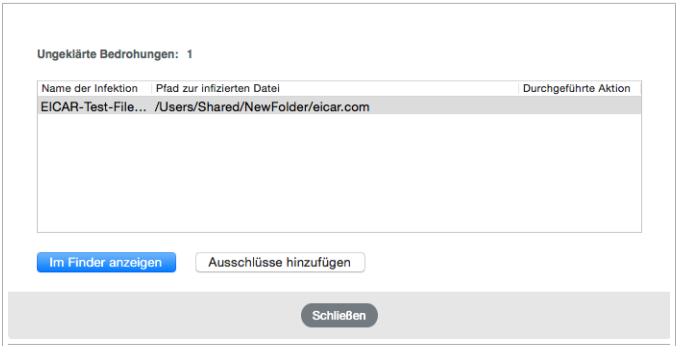
Beheben Sie die in Bitdefender Antivirus for Mac angezeigten Probleme, um schnell und einfach den optimalen Schutz für Ihr System und Ihre Daten sicherzustellen.

Zu den erkannten Problemen gehören:

- Neue Informationen zu Bedrohungen und Produkt-Updates wurden nicht von unseren Servern heruntergeladen, da der **Autopilot** deaktiviert ist.
- In Ihrem System wurden nicht beseitigte Bedrohungen gefunden.
- **Autopilot** ist ausgeschaltet.

Um erkannte Probleme zu überprüfen und zu beheben:

1. Öffnen Sie Bitdefender Antivirus for Mac.
2. Liegen keine Warnungen in Bitdefender vor, ist die Statusleiste grün. Wenn ein Sicherheitsproblem gefunden wurde, ändert die Statusleiste ihre Farbe auf gelb.
3. Überprüfen Sie die Beschreibung für weitere Informationen.
4. Wenn ein Sicherheitsproblem gefunden wurde, können Sie mit einem Klick auf die Schaltfläche **Probleme anzeigen** die Probleme anzeigen, die die Sicherheit Ihres Systems gefährden. Im daraufhin angezeigten Fenster können Sie verschiedene Aktionen wählen.




Fenster mit nicht beseitigten Bedrohungen

Die Liste der nicht beseitigten Bedrohungen wird nach jedem System-Scan aktualisiert.

Für nicht beseitigte Bedrohungen sind die folgenden Aktionen verfügbar:

- Im Finder zeigen. Mit dieser Aktion können Sie Infektionen manuell entfernen.
- Ausnahmen hinzufügen. Diese Aktion ist nicht für Bedrohungen verfügbar, die innerhalb von Archiven gefunden wurden.

## 9.7. Internet-Schutz

Bitdefender Antivirus for Mac verwendet die TrafficLight-Erweiterungen, um Ihnen ein sicheres Surfen im Web zu ermöglichen. Die TrafficLight-Erweiterungen lesen, verarbeiten und filtern den gesamten Datenverkehr und blockieren dabei alle schädlichen Inhalte.

Die Erweiterungen lassen sich in die folgenden Browser integrieren: Mozilla Firefox, Google Chrome and Safari.

### Aktivierung von Linkchecker-Erweiterungen

Um die Linkchecker-Erweiterungen zu aktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie Bitdefender Antivirus for Mac.
2. Klicken Sie auf **Jetzt lösen**, um den Internet-Schutz zu aktivieren.

3. Bitdefender Antivirus for Mac erkennt, welcher Web-Browser auf Ihrem System installiert ist. Um die Linkchecker-Erweiterung zu installieren, klicken Sie auf **Erweiterung herunterladen**.
4. Sie werden an folgende Internet-Adresse weitergeleitet:

   https://www.bitdefender.com/solutions/trafficlight.html
5. Wählen Sie hier **Kostenloser Download**.
6. Folgen Sie den Anweisungen, um die Linkchecker-Erweiterung für Ihren Browser zu installieren.

## Verwalten von Erweiterungseinstellungen

Ihnen steht eine große Auswahl an Funktionen zur Verfügung, die Sie vor allen möglichen Bedrohungen im Internet schützen. Sie können sie aufrufen, indem Sie auf das TrafficLight-Symbol neben Ihren Browser-Einstellungen und danach auf **Einstellungen** klicken:

- **Bitdefender-TrafficLight-Einstellungen**
  - Hochentwickelter Bedrohungsfilter - Verhindert, dass Sie Websites aufrufen, die zur Verbreitung von Malware sowie von Phishing- und Betrugsversuchen eingesetzt werden.
  - Tracker-Erkennung - Erkennt Tracker auf besuchten Webseiten und informiert Sie entsprechend.
  - Suchergebnisanalyse - Warnt Sie schon in Ihren Suchergebnissen vor gefährlichen Websiten.

    Wenn alle Einstellungen deaktiviert sind, werden keine Websites gescannt.
- **Whitelist**

  Websites können von der Prüfung durch die Bitdefender-Engines ausgeschlossen werden. Geben Sie dazu in das entsprechende Feld den Namen der Website ein, die Sie zur Whitelist hinzufügen möchten, und klicken Sie auf **HINZUFÜGEN**.

  Es wird keine Warnmeldung mehr angezeigt, auch wenn von den ausgeschlossenen Seiten eine Bedrohung ausgeht. Sie sollten dieser Liste nur Website hinzufügen, denen Sie uneingeschränkt vertrauen.

### Seitenbewertung und Warnungen

Abhängig von der Linkchecker-Einstufung für die Webseite, die sie gerade besuchen, wird eines der folgenden Symbole in diesem Bereich eingeblendet:

Diese Seite ist sicher. Sie können mit Ihrer Arbeit fortfahren.
Diese Webseite könnte gefährliche Inhalte haben. Seien Sie vorsichtig, wenn Sie sie dennoch aufrufen möchten.
Sie sollten die Webseite umgehend verlassen, da diese Malware oder andere Bedrohungen enthält.

In Safari sind die TrafficLight-Symbole schwarz hinterlegt.

## 9.8. Updates

Jeden Tag werden neue Bedrohungen entdeckt und identifiziert. Deshalb ist es so wichtig, Bitdefender Antivirus for Mac über Updates ständig auf dem neuesten Stand zu halten.

Der **Autopilot** sollte immer aktiviert bleiben, damit Informationen zu Bedrohungen und Produkt-Updates jederzeit automatisch heruntergeladen werden können. Wenn ein neues Update erkannt wird, wird es automatisch auf Ihren PC heruntergeladen und installiert.

Die Aktualisierung der Bedrohungsinformationen wird „on the fly" durchgeführt. Das bedeutet, dass die zu aktualisierenden Dateien schrittweise ersetzt werden. So stört das Update nicht den Betrieb des Produkts, während gleichzeitig alle Schwachstellen behoben werden.

- Wenn Bitdefender Antivirus for Mac up-to-date ist, spürt die Software die neuesten Threats auf und heilt infizierte Dateien.
- Ist Bitdefender Antivirus for Mac nicht auf dem neuesten Stand, kann es die neusten, von den Bitdefender-Laboren entdeckten Bedrohungen nicht erkennen und entfernen.

### 9.8.1. Benutzergesteuertes Update

Ein manuelles Update können Sie jederzeit durchführen.

Für regelmäßige Updates und Downloads ist eine aktive Internetverbindung nötig.

Führen Sie folgende Schritte für ein manuelles Update durch:

1. Öffnen Sie Bitdefender Antivirus for Mac.

2. Klicken Sie auf die Schaltfläche **Aktionen** in der Menüleiste.
3. Klicken Sie auf **Virendatenbank aktualisieren**.

Alternativ können Sie ein Update auch manuell anfordern, indem Sie CMD + U drücken.

Der Update-Fortschritt und die heruntergeladenen Dateien werden eingeblendet.

### 9.8.2. Updates über einen Proxy Server

Bitdefender Antivirus for Mac kann Updates über einen Proxy Server nur dann durchführen, wenn dafür keine Autorisierung notwendig ist. Sie müssen keine Programmeinstellungen konfigurieren.

Wenn Ihre Internetverbindung über einen Proxy-Server läuft, der eine Autorisierung verlangt, müssen Sie regelmäßig zu einer direkten Internetverbindung wechseln, um die neuesten Bedrohungsinformationen herunterladen zu können.

### 9.8.3. Upgrade auf eine neue Version durchführen

Von Zeit zu Zeit veröffentlichen wir Produkt-Updates, die neue Funktionen bringen oder bestimmte Aspekte der Software verbessern oder Probleme beheben. Bei diesen Updates kann es notwendig werden, das System neu zu starten, um die Installation neuer Dateien zu ermöglichen. Falls ein Update einen Neustart erforderlich macht, wird Bitdefender Antivirus for Mac standardmäßig bis zum Neustart des Systems die bereits vorhandenen Dateien nutzen. So beeinträchtigt der Aktualisierungsprozess den Benutzer nicht bei seiner Arbeit.

Ein Pop-up-Fenster fordert Sie auf das System neu zu starten, sobald das Update abgeschlossen wurde. Fall Sie diese Benachrichtigung verpassen, können Sie das System manuell neu starten oder in der Menüleiste auf **Für das Upgrade neu starten** klicken.

### 9.8.4. Informationen zu Bitdefender Antivirus for Mac finden

Informationen zur installierten Bitdefender Antivirus for Mac-Version finden Sie im Bereich **Info über**. Hier können Sie die Abonnementvereinbarung sowie die Datenschutzerklärung aufrufen und lesen sowie die Open-Source-Lizenzen anzeigen.

So rufen Sie das Fenster „Über“ auf:

1. Öffnen Sie Bitdefender Antivirus for Mac.
2. Klicken Sie in der Menüleiste auf Bitdefender Antivirus for Mac und wählen Sie **Über Antivirus for Mac**.

# 10. EINSTELLUNGEN KONFIGURIEREN

Dieses Kapital beinhaltet die folgenden Themen:


- *„Zugriff auf Einstellungen“* (S. 257)
- *„Kontodetails“* (S. 257)
- *„Schutzeinstellungen“* (S. 258)
- *„Prüfausnahmen“* (S. 259)
- *„Sichere Dateien“* (S. 260)
- *„Verlauf“* (S. 263)
- *„Quarantäne“* (S. 264)


## 10.1. Zugriff auf Einstellungen

Um das Präferenzen-Fenster von Bitdefender Antivirus for Mac zu öffnen:

1. Öffnen Sie Bitdefender Antivirus for Mac.
2. Wählen Sie eine der folgenden Methoden:
   - Klicken Sie in der Menüleiste auf Bitdefender Antivirus for Mac und wählen Sie **Präferenzen**.
   - Klicken Sie in der Menüleiste auf das Symbol und wählen Sie **Einstellungen**.
   - Drücken Sie Befehl-Komma (,).

## 10.2. Kontodetails

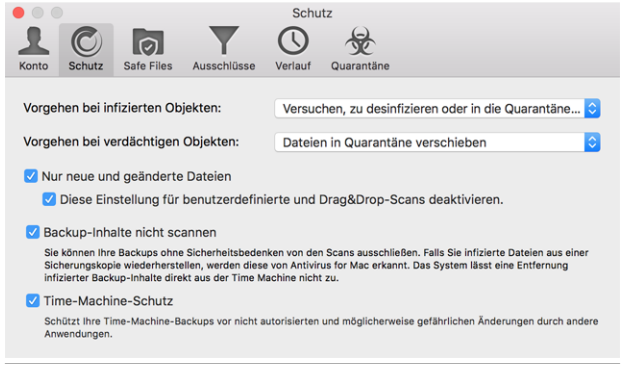
Das Fenster Kontoinformationen enthält Informationen zu Ihrem Abonnement und Ihrem Bitdefender-Konto.

Wenn Sie sich mit einem anderen Bitdefender-Konto anmelden möchten, klicken Sie auf die Schaltfläche **Konto wechseln**, geben Sie die neue E-Mail-Adresse und das Passwort in das Bitdefender-Konto Fenster ein und klicken Sie anschließend auf **EINLOGGEN**.

In diesem Fenster können Sie auch die Option **Meine Angebote** aktivieren oder deaktivieren. Wenn sie aktiviert ist, wird jedes Mal ein Hinweis angezeigt, wenn Bitdefender ein besonderes Angebot für Sie hat.

## 10.3. Schutzeinstellungen

Über das Schutzeinstellungsfenster können Sie den gesamten Scan-Vorgang konfigurieren. Sie können die Aktionen, die bei infizierten oder verdächtigen Dateien vorgenommen werden sollen oder auch allgemeine Einstellungen konfigurieren.




Schutzeinstellungen

- **Vorgehen bei infizierten Objekten.** Wenn Bitdefender Antivirus for Mac eine Bedrohung erkennt, versucht das Programm automatisch den Schad-Code der infizierten Datei zu entfernen und die Originaldatei wiederherzustellen. Diese Operation bezeichnet man als Desinfektion. Dateien, die nicht desinfiziert werden können, werden in die Quarantäne verschoben, um so die Infizierung einzudämmen.

  Obwohl wir dies nicht empfehlen, können Sie die Anwendung so einstellen, dass für infizierte Dateien keine Aktionen durchgeführt werden. Erkannte Dateien werden nur protokolliert.

  Der Autopilot stellt sicher, dass Ihr System vor Bedrohungen geschützt ist, und hat dabei nur minimale Auswirkungen auf die Systemleistung. Sollten nicht beseitigte Bedrohungen vorliegen, können Sie diese anzeigen und über Ihr weiteres Vorgehen entscheiden.

- **Vorgehen bei verdächtigen Objekten.** Dateien werden von der heuristischen Analyse als verdächtig klassifiziert. Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist.

  Verdächtige Dateien werden standardmäßig in die Quarantäne verschoben. Bedrohungen in Quarantäne können keinen Schaden anrichten, da sie dort nicht geöffnet oder ausgeführt werden können.

  Optional können Sie verdächtige Dateien auch ignorieren. Erkannte Dateien werden nur protokolliert.

- **Nur neue und geänderte Dateien.** Aktivieren Sie diese Option, wenn Bitdefender Antivirus for Mac nur Dateien prüfen soll, die vorher noch nicht geprüft wurden oder die seit dem letzten Scan modifiziert wurden.

  Sie können wählen, dass diese Einstellung für das drag und drop-Scanning nicht angewandt wird, wenn Sie das entsprechende Kästchen anklicken.

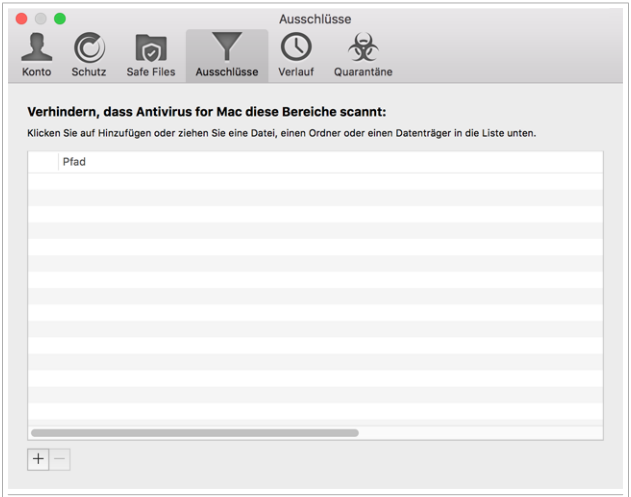
- **Backup-Inhalte nicht scannen.** Markieren Sie dieses Kästchen, um Backup-Dateien vom Scan auszuschließen. Werden infizierte Dateien zu einem späteren Zeitpunkt wiederhergestellt, erkennt Bitdefender Antivirus for Mac diese automatisch und leitet geeignete Maßnahmen ein.

- **Time-Machine-Schutz.** Aktivieren Sie dieses Kästchen, um die Dateien in der Time Machine zu schützen. Werden Dateien in Ihrem Time-Machine-Laufwerk von Ransomware verschlüsselt, können Sie sie auch ohne Lösegeldzahlung wiederherstellen.

### 10.3.1. Prüfausnahmen

Wenn Sei möchten können Sie Bitdefender Antivirus for Mac so einstellen, dass spezielle Dateien, Ordner oder auch ein ganzer Laufwerke, nicht gescannt werden. Zum Beispiel könnten Sie vom Scannen ausschließen:

- Dateien die fälschlicherweise als infiziert identifiziert wurden (bekannt als "false positives")
- Dateien die Scanfehler verursachen
- Backup-Laufwerke




Prüfausnahmen

Die Ausnahmeliste enthält den Pfad der vom Scannen ausgenommen wurde.

Es gibt zwei Wege um eine Scan-Ausnahme einzurichten:

- Die gewünschte Datei, den Ordner oder das Laufwerk per Drag&drop in die Ausnahmeliste ziehen.
- Klicken Sie auf den Button mit dem Plus-Zeichen (+), der sich unter der Ausschlußliste befindet. Wählen Sie dann die Datei, den Ordner oder das Laufwerk, das vom Scan ausgeschlossen werden soll.

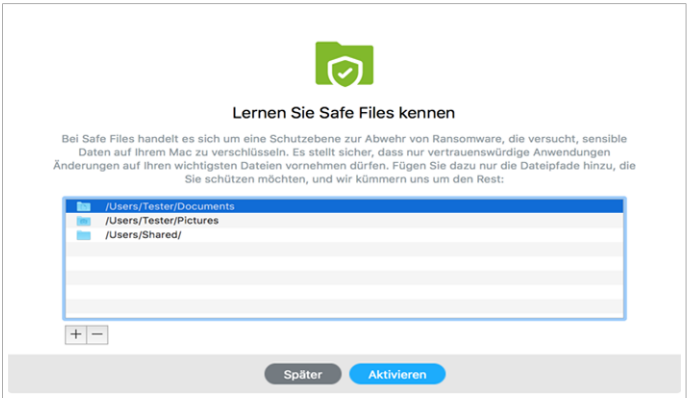
Um eine Scan-Ausnahme zu entfernen, wählen Sie den entsprechenden Eintrag aus der Liste und klicken Sie auf den Button mit dem Minuszeichen (-) unter der Ausnahmeliste.

## 10.4. Sichere Dateien

Bei Ransomware handelt es sich um Schadsoftware, die anfällige Systeme infiziert und den Zugriff darauf sperrt. Von den Benutzern wird dann für die

Freigabe ihrer Daten ein Lösegeld erpresst. Diese Schadsoftware geht intelligent vor und zeigt Benutzern gefälschte Warnmeldungen an, um sie in Angst zu versetzen und sie dazu zu bringen, das geforderte Geld zu zahlen.

Durch den Einsatz neuester Technologien stellt Bitdefender die Integrität des System sicher. Kritische Systembereiche werden vor Ransomware-Angriffen geschützt, ohne dabei das System zu beeinträchtigen. Um zu verhindern, dass nicht vertrauenswürdige Anwendungen auf Ihre Dokumente, Fotos oder Videos zugreifen, bietet Ihnen Bitdefender Safe Files Ihnen die Möglichkeit, Ihre persönlichen Dateien zu beschützen und selbst festzulegen, welche Apps autorisiert sind, Änderungen an geschützten Dateien vorzunehmen.




Safe-Files-Assistent

Der Assistent für Bitdefender Safe Files wird angezeigt, sobald Sie Bitdefender Antivirus for Mac auf Ihrem Macintosh installieren. Wählen Sie die zu schützenden Speicherorte aus oder fügen Sie neue hinzu und klicken Sie danach auf **Safe Files aktivieren**.

Sichere Dateien

Zum späteren Hinzufügen weiterer Dateien zur geschützten Umgebung gibt es zwei Optionen:

- Verschieben Sie eine Datei, einen Ordner oder ein Laufwerk per Drag&Drop in das Safe-Files-Fenster.
- Klicken Sie auf das Plus-Zeichen (+) unterhalb der Liste mit den geschützten Dateien. Wählen Sie danach die Datei, den Ordner oder das Laufwerk aus, das Sie vor dem Zugriff durch Ransomware schützen möchten.

Um Systembeeinträchtigungen zu vermeiden, sollten Sie nicht mehr als 30 Ordner hinzufügen oder mehrere Dateien in einem Ordner speichern.

Die Ordner Bilder, Dokumente, Desktop und Downloads werden standardmäßig vor Angriffen geschützt.

**Beachten Sie**

Benutzerdefinierte Ordner können nur für den aktuellen Benutzer geschützt werden. Externe Laufwerke sowie System- und Anwendungsdateien können der Schutzumgebung nicht hinzugefügt werden.

Sie werden informiert, sobald eine unbekannte Anwendung mit ungewöhnlichen Verhalten versucht, die von Ihnen hinzugefügten Dateien

zu verändern. Klicken Sie auf **Zulassen** oder **Blockieren**, um sie zur Liste der verwalteten Anwendungen hinzuzufügen.

### 10.4.1. Verwalten von Anwendungen

Anwendungen, die versuchen, geschützte Dateien zu verändern oder zu löschen, können als potenziell unsicher markiert und zur Liste der blockierten Anwendungen hinzugefügt werden. Falls eine solche Anwendung blockiert wird und Sie sich sicher sind, dass ihr Verhalten keinen Anlass zur Sorge gibt, können Sie die Ausführung der Anwendung zulassen, indem Sie auf **Anwendungen verwalten** klicken und den Status auf Zulassen setzen.

Ebenso können Sie den Status zugelassener Anwendungen auf blockiert setzen.

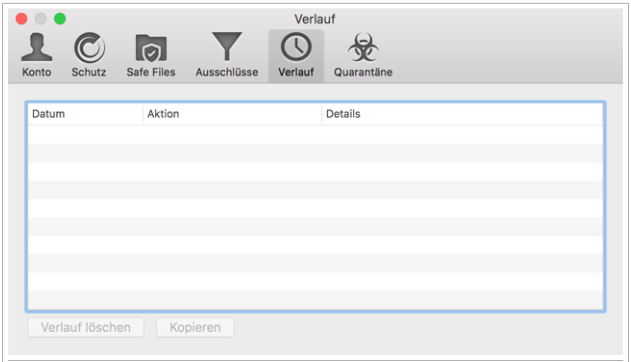
Nutzen Sie Drag&Drop oder klicken Sie auf das Pluszeichen (+), um weitere Apps zur Liste hinzuzufügen.

## 10.5. Verlauf

Bitdefender führt ein detailliertes Ereignisprotokoll über alle Aktivitäten der Software auf Ihrem Computer. Alle Ereignisse, die sich auf Ihr System oder Ihre Daten auswirken, werden als neue Nachricht in den Bitdefender Antivirus for Mac-Verlauf aufgenommen, in etwa wie eine neue E-Mail, die in einem Postfach eingeht.

Ereignisse sind ein wichtiges Hilfsmittel für die Überwachung und Verwaltung Ihres Bitdefender-Schutzes. So können Sie beispielsweise einfach überprüfen, ob ein Update erfolgreich durchgeführt wurde, ob eine Bedrohung auf Ihrem Computer entdeckt wurde, ob eine nicht autorisierte Anwendung auf Ihr Time-Machine-Laufwerk zugreifen wollte usw.

Details zu den Produktaktivitäten werden angezeigt.



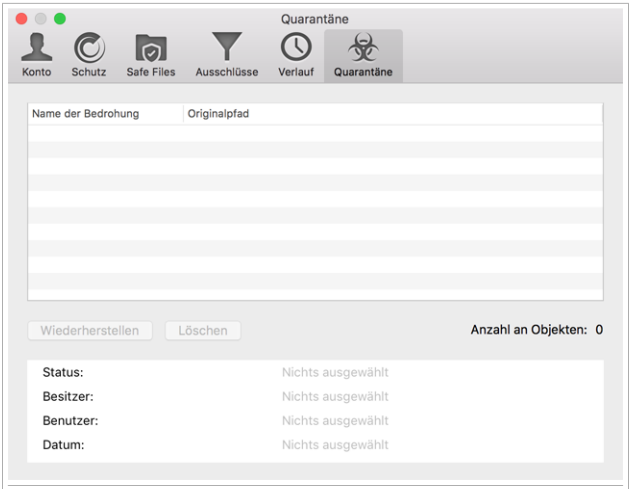

Verlauf

Wenn Sie den Protokollverlauf löschen möchten, klicken Sie auf die Schaltfläche **Verlauf löschen**.

Mithilfe der Schaltfläche **Kopieren** können Sie diese Informationen in die Zwischenablage kopieren.

## 10.6. Quarantäne

Mit Bitdefender Antivirus for Mac können infizierte oder verdächtige Dateien in einem sicheren Bereich, der Quarantäne, isoliert werden. Bedrohungen in Quarantäne können keinen Schaden anrichten, da sie dort nicht geöffnet oder ausgeführt werden können.




Dateien in Quarantäne

Der Bereich Quarantäne zeigt alle Dateien an, die sich zur Zeit im Quarantäne-Ordner befinden.

Um eine Datei aus der Quarantäne zu löschen, markieren Sie diese und klicken Sie dann auf **Löschen**. Wenn Sie eine Quarantäne-Datei am ursprünglichen Speicherort wiederherstellen möchten, klicken Sie zuerst auf die Datei und dann auf **Wiederherstellen**.

# 11. VPN

Dieses Kapital beinhaltet die folgenden Themen:


- *„Über VPN“* (S. 266)
- *„VPN installieren“* (S. 266)
- *„Öffnen des VPN“* (S. 267)
- „VPN-Benutzeroberfläche“ (S. 267)
- *„Abonnements“* (S. 287)


## 11.1. Über VPN

Mit Bitdefender VPN schützen Sie Ihre Daten bei Verbindungen mit ungesicherten WLAN-Netzwerken wie zum Beispiel in Flughäfen, Einkaufszentren, Cafés oder Hotels. So vermeiden Sie unglückliche Situationen wie den Diebstahl Ihrer persönlichen Daten oder Versuche, Ihre Geräte-IP-Adresse für Hacker offenzulegen.

Das VPN dient als Tunnel zwischen Ihrem Gerät und dem Netzwerk, mit dem Sie sich verbinden. Ihre Verbindung wird abgesichert, Ihren Daten werden professionell nach Bankenstandard verschlüsselt und Ihre IP-Adresse bleibt jederzeit unsichtbar. Ihr Datenverkehr wird über spezielle Server weitergeleitet, was es nahezu unmöglich macht, Ihr Gerät neben den unzähligen anderen Geräten zu identifizieren, die ebenfalls unsere Dienste in Anspruch nehmen. Darüber hinaus können Sie mit Bitdefender VPN im Internet auch auf solche Inhalte zugreifen, die üblicherweise regionalen Zugangsbeschränkungen unterliegen.

### Beachten Sie

In manchen Ländern wird Internetzensur betrieben. Aus diesem Grund ist die Nutzung von VPNs hier gesetzlich verboten. Um rechtliche Konsequenzen zu vermeiden, wird Ihnen bei der ersten Nutzung der Bitdefender-VPN-App eine Warnmeldung angezeigt. Durch die weitere Nutzung der App bestätigen Sie, dass Sie sich aller einschlägigen Rechtsvorschriften in Ihrem Land sowie der möglichen Risiken, denen Sie sich aussetzen, bewusst sind.

## 11.2. VPN installieren

Die VPN-App kann über das Bitdefender-Hauptfenster wie im Folgenden beschrieben installiert werden:

1. Öffnen Sie Bitdefender Antivirus for Mac.
2. Klicken Sie unten rechts auf **Hol es dir jetzt.**
3. Lesen Sie in den Fenster, in dem die VPN-App beschrieben wird, die **Abonnementvereinbarung** durch und klicken Sie danach auf **VPN installieren**. Falls die den Bedingungen der Vereinbarung nicht zustimmen, klicken Sie zum Abbruch der Installation auf **Später**.
4. Klicken Sie zum Abschluss des Installationsvorgangs auf **Verstanden**.

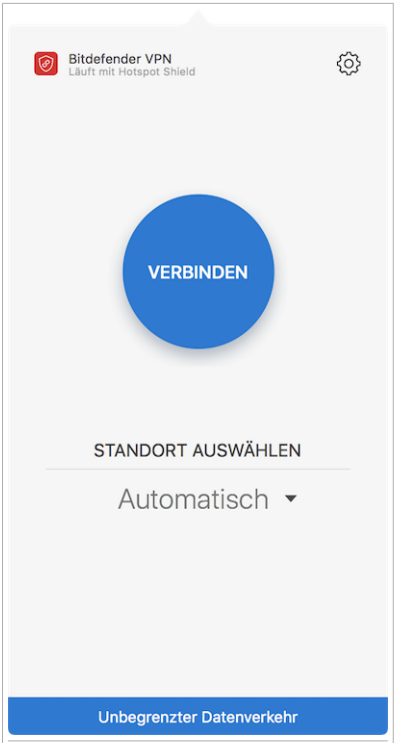
## 11.3. Öffnen des VPN

Wenn Sie die Bitdefender-VPN-App öffnen möchten, klicken Sie auf das Symbol in der Menüleiste. Alternativ können Sie den Ordner Programme öffnen, dann den Ordner Bitdefender öffnen und dann auf das Symbol Bitdefender VPN doppelklicken.

## 11.4. Netzwerkkarte

In der VPN-Benutzeroberfläche wird der Status der App angezeigt, verbunden oder getrennt. Der Serverstandort wird für Anwender mit der kostenlosen Version von Bitdefender automatisch auf den geeignetsten Server festgelegt. Premium-Anwender können den Serverstandort selbst wählen, indem sie ihn aus der Liste **STANDORT AUSWÄHLEN** auswählen. Weitere Einzelheiten zu den VPN-Abonnments finden Sie unter *„Abonnements“ (S. 287)*.

Klicken Sie auf die Statusanzeige oben im Bild, um die Verbindung herzustellen oder zu trennen. Ein schwarzes Symbol in der Menüleiste zeigt an, dass eine Verbindung besteht. Ist das Symbol weiß, wurde die Verbindung getrennt.




VPN-Benutzeroberfläche

Während die Verbindung besteht, wird die verstrichene Zeit unten in der Benutzeroberfläche angezeigt. Klicken Sie oben rechts auf das ⚙-Symbol, um auf weitere Optionen zuzugreifen.

- **Mein Konto** - Hier finden Sie Details zu Ihrem Bitdefender-Benutzerkonto und Ihrem VPN-Abonnement. Klicken Sie auf **Konto wechseln**, wenn Sie sich mit einem anderen Konto anmelden möchten.
- **Einstellungen** - Hier können Sie das Produktverhalten individuell anpassen:
  - Legen Sie fest, dass das VPN beim Systemstart ausgeführt wird
  - Erhalten Sie Benachrichtigungen, wenn das VPN Verbindungen automatisch herstellt oder trennt
- **Upgrade zur Premium-Version** - Falls Sie die kostenlose Produktversion nutzen, können Sie hier auf die Premium-Version upgraden. Klicken Sie

**JETZT UPGRADEN**, um auf eine Webseite weitergeleitet zu werden, über die Sie ein Abonnement erwerben können.

- **Support** - Sie werden auf die Support Center-Platform weitergeleitet, wo Sie einen hilfreichen Artikel zur Nutzung der Bitdefender VPN lesen können.
- **Über** - Hier finden Sie Informationen zur installierten Version.
- **Beenden** - hiermit verlassen Sie die Anwendung.

## 11.5. Abonnements

Mit Bitdefender VPN erhalten Sie ein kostenloses Datenvolumen von 200 MB pro Tag, um Ihre Verbindung bei Bedarf abzusichern. Sie werden automatisch mit dem besten Serverstandort verbunden.

Wenn Sie sich für ein Upgrade auf die Premium-Version entscheiden, entfällt das Datenlimit und Sie können durch die freie Wahl des Serverstandorts Inhaltsbeschränkungen überall auf der Welt umgehen.

Mit einem Klick auf **UNBEGRENZTER DATENVERKEHR** können Sie über die Benutzeroberfläche jederzeit ein Upgrade auf Bitdefender Premium VPN durchführen.

Ein Bitdefender Premium-VPN-Abonnement läuft unabhängig von dem Bitdefender Antivirus for Mac-Abonnement, d. h. Sie können es über den gesamten Verfügbarkeitszeitraum hinweg nutzen, unabhängig von Status Ihres Sicherheitsabonnement Wenn Ihr Bitdefender Premium-VPN-Abonnement abläuft, Ihr Bitdefender Antivirus for Mac-Abonnement aber weiterhin aktiv ist, kehren Sie zum kostenlosen Angebot zurück.

Bitdefender VPN ist ein plattformübergreifendes Produkt, das in Bitdefender-Produkten für Windows, macOS, Android und iOS verfügbar ist. Nach einem Premium-Upgrade können Sie Ihr Abonnement in allen Produkten nutzen, vorausgesetzt, dass Sie sich mit dem gleichen Bitdefender-Benutzerkonto anmelden.

# 12. BITDEFENDER CENTRAL

Dieses Kapital beinhaltet die folgenden Themen:

- *„Über Bitdefender Central“* (S. 270)
- *„Meine Abonnements“* (S. 271)
- *„Meine Geräte“* (S. 272)

## 12.1. Über Bitdefender Central

Bitdefender Central stellt Ihnen eine Web-Plattform zur Verfügung, über die Sie auf die Online-Funktionen und -Dienste des Produkts zugreifen und wichtige Aufgaben auf allen Geräten ausführen können, auf denen Bitdefender installiert ist. Über https://central.bitdefender.com können Sie sich mit jedem internetfähigen Computer oder Mobilgerät bei Ihrem Bitdefender-Konto anmelden. Nachdem Sie es aufgerufen haben, stehen Ihnen die folgenden Optionen zur Verfügung:

- Laden Sie Bitdefender herunter und installieren Sie es auf Windows-, macOS-, iOS- und Android-Betriebssystemen. Die folgenden Produkte stehen zum Download bereit:
  - Bitdefender Antivirus for Mac
  - Die Bitdefender-Windows-Produktlinie
  - Bitdefender Mobile Security für Android
  - Bitdefender Mobile Security for iOS
  - Bitdefender-Elternratgeber
- Verwaltung und Verlängerung Ihrer Bitdefender-Abonnements.
- Neue Geräte zu Ihrem Netzwerk hinzufügen und diese Geräte aus der Ferne verwalten.

## 12.2. So können Sie Bitdefender Central aufrufen:

Bitdefender Central kann auf verschiedene Weise aufgerufen werden. Je nach durchzuführender Aufgabe stehen Ihnen die folgenden Optionen zur Verfügung:

- Über das Bitdefender Antivirus for Mac-Hauptfenster:

1. Klicken Sie rechts unten in der Benutzeroberfläche auf den Link **Zum eigenen Konto**.

- Über Ihren Web-Browser:
  1. Öffnen Sie einen Web-Browser auf jedem beliebigen internetfähigen Gerät.
  2. Gehen Sie zu: https://central.bitdefender.com.
  3. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Konto an.

## 12.3. Meine Abonnements

Über die Bitdefender Central-Plattform können Sie bequem die Abonnements für alle Ihre Geräte verwalten.

### 12.3.1. Abonnement aktivieren

Sie können Ihr Abonnement während des Installationsvorgangs mithilfe Ihres Bitdefender-Kontos aktivieren. Sobald die Aktivierung abgeschlossen ist, beginnt die Laufzeit des Abonnements.

Falls Sie einen Aktivierungscode von einem unserer Wiederverkäufer gekauft oder diesen als Geschenk erhalten haben, können Sie die Gültigkeitsdauer Ihres Bitdefender-Abonnements um diesen Zeitraum verlängern.

So können Sie Ihr Abonnement mit einem Aktivierungscode aktivieren:

1. Rufen Sie Bitdefender Central auf.
2. Klicken Sie oben links im Fenster auf das ☰-Symbol und öffnen Sie den Bereich **Meine Abonnements**.
3. Klicken Sie auf **AKTIVIERUNGSCODE** und geben Sie den Code in das entsprechende Feld ein.
4. Klicken Sie zum Fortfahren auf **AKTIVIEREN**.

Das Abonnement wurde aktiviert.

Informationen zur Installation des Produktes auf Ihren Geräten finden Sie im Abschnitt *„Installation von Bitdefender Antivirus for Mac“ (S. 236)*.

### 12.3.2. Abonnement abschließen

So können Sie ein Abonnement direkt über Ihr Bitdefender-Benutzerkonto erwerben:

1. Rufen Sie Bitdefender Central auf.
2. Klicken Sie oben links im Fenster auf das ☰-Symbol und öffnen Sie den Bereich **Meine Abonnements**.
3. Klicken Sie auf **Jetzt kaufen**. Sie werden auf eine Webseite weitergeleitet, auf der Sie den Kauf tätigen können.

Sofort nach Abschluss des Vorgangs wird die Verfügbarkeit des Abonnements unten rechts im Hauptfenster des Produkts angezeigt.

## 12.4. Meine Geräte

Über Ihr Bitdefender-Benutzerkonto können Sie im Bereich **Meine Geräte** die Bitdefender-Produkte auf Ihren Geräten aus der Ferne installieren und verwalten, sofern die Geräte eingeschaltet und mit dem Internet verbunden sind. Auf den Gerätekacheln sind der Gerätename, der Sicherheitsstatus angegeben sowie die Information, ob Sicherheitsprobleme auf Ihren Geräten bestehen.

### 12.4.1. Persönliche Anpassungen

Sie können Gerätenamen vergeben, um die Geräte später leichter identifizieren zu können:

1. Rufen Sie Bitdefender Central auf.
2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie auf die gewünschte Gerätekachel und dann auf das Symbol ⋮ in der rechten oberen Ecke.
4. Tippen Sie auf **Einstellungen**.
5. Geben Sie einen neuen Namen in das Feld **Gerätename** ein und clicken Sie dann auf **SPEICHERN**.

Sie können für jedes Ihrer Geräte zur einfacheren Verwaltung einen Besitzer anlegen und zuordnen:

1. Rufen Sie Bitdefender Central auf.

2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie auf die gewünschte Gerätekachel und dann auf das Symbol
   in der rechten oberen Ecke.
4. Wählen Sie **Profil**.
5. Klicken Sie auf **Besitzer hinzufügen** und füllen Sie dann die entsprechenden Felder aus. Passen Sie das Profil nach Bedarf an, indem Sie ein Foto hinzufügen, einen Geburtstag auswählen und eine E-Mail-Adresse sowie eine Telefonnummer eingeben.
6. Klicken Sie auf **HINZUFÜGEN**, um das Profil zu speichern.
7. Wählen Sie aus der **Gerätebesitzer**-Liste den gewünschten Besitzer aus und klicken Sie auf **ZUORDNEN**.

### 12.4.2. Fernzugriffsaktionen

So können Sie Bitdefender per Fernzugriff auf Ihren Geräten aktualisieren:

1. Rufen Sie Bitdefender Central auf.
2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie auf die gewünschte Gerätekachel und dann auf das Symbol
   in der rechten oberen Ecke.
4. Wählen Sie **Update**.

So können Sie den Autopilot per Fernzugriff aktivieren:

1. Rufen Sie Bitdefender Central auf.
2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie auf die gewünschte Gerätekachel und dann auf das Symbol
   in der rechten oberen Ecke.
4. Tippen Sie auf **Einstellungen**. Klicken Sie auf den entsprechenden Schalter, um den Autopiloten zu aktivieren.

Klicken Sie auf eine Gerätekarte, um die folgenden Reiter anzuzeigen:

- **Dashboard** . In diesem Fenster können Sie Details zum ausgewählten Gerät anzeigen, den Schutzstatus sowie die Zahl der blockierten Bedrohungen der letzten sieben Tage einsehen. Der Sicherheitsstatus ist grün, wenn es keine Sicherheitsprobleme gibt, gelb, wenn es etwas gibt, was Ihre

Aufmerksamkeit erfordert, und rot, wenn Ihr Gerät gefährdet ist. Gibt es Probleme, die sich auf Ihr Gerät auswirken, klicken Sie im oberen Statusbereich auf den Drop-down-File, um weitere Details anzuzeigen. Von hier aus können die Probleme, die Ihre Gerätesicherheit beeinträchtigen, manuell behoben werden.

- **Schutz**. Von diesem Fenster aus können Sie einen Quick Scan oder einen Vollständiger Scan auf Ihren Geräten durchführen. Klicken Sie auf **SCAN**, um den Vorgang zu starten. Sie können auch nachvollziehen, wann der letzte Scan auf dem Gerät durchgeführt wurde, und einen Bericht für den aktuellsten Scan abrufen, in dem die wichtigsten Informationen zusammengefasst werden. Details zu diesen beiden Scan-Arten finden Sie unter „*Ihren Mac scannen*“ (S. 247).

# 13. HÄUFIG GESTELLTE FRAGEN

**Wie kann ich Bitdefender Antivirus for Mac testen, bevor ich ein Abonnement abschließe?**

Sie sind ein neuer Bitdefender-Kunde und möchten unser Produkt testen, bevor Sie es kaufen. Der Testzeitraum beträgt 30 Tage. Nach Ablauf dieser Frist können Sie das Produkt nur weiterverwenden, wenn Sie ein Bitdefender-Abonnement erwerben. So erhalten Sie die Bitdefender Antivirus for Mac-Testversion:

1. Erstellen Sie ein Bitdefender-Konto wie folgt:
   - Gehen Sie zu: https://central.bitdefender.com.
   - Geben Sie die erforderlichen Informationen in die entsprechenden Felder ein und klicken Sie auf **BENUTZERKONTO ANLEGEN**.

     Die hier eingetragenen Daten bleiben vertraulich.
2. Laden Sie Bitdefender Antivirus for Mac wie folgt herunter:
   - Rufen Sie den Bereich **Meine Geräte** auf und klicken Sie auf **LOKALEN SCHUTZ INSTALLIEREN**.
   - Wählen Sie eine der beiden verfügbaren Optionen:
     - **HERUNTERLADEN**

       Klicken Sie auf die Schaltfläche und speichern Sie die Installationsdatei.
     - **Auf einem anderen Gerät**

       Wählen Sie **macOS** aus, um Ihr Bitdefender-Produkt herunterzuladen und klicken Sie danach auf **FORTFAHREN**. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **SENDEN**.
   - Führen Sie das von Ihnen heruntergeladene Bitdefender aus.

**Ich habe einen Aktivierungscode. Wie verlängere ich damit die Laufzeit meines Abonnements?**

Falls Sie einen Aktivierungscode von einem unserer Wiederverkäufer gekauft oder diesen als Geschenk erhalten haben, können Sie die Gültigkeitsdauer Ihres Bitdefender-Abonnements um diesen Zeitraum verlängern.

So können Sie Ihr Abonnement mit einem Aktivierungscode aktivieren:

1. Rufen Sie Bitdefender Central auf.
2. Klicken Sie oben links im Fenster auf das -Symbol und öffnen Sie den Bereich **Meine Abonnements**.
3. Klicken Sie auf **AKTIVIERUNGSCODE** und geben Sie den Code in das entsprechende Feld ein.
4. Klicken Sie zum Fortfahren auf **AKTIVIEREN**.

Die Erweiterung wird jetzt in Ihrem Bitdefender-Konto sowie im rechten unteren Bereich der Oberfläche Ihres installierten Bitdefender Antivirus for Mac-Produkts angezeigt.

**Das Scan-Protokoll zeigt bisher noch nicht gelöste Probleme. Wie kann ich diese beheben?**

Mögliche noch nicht gelöste Probleme im Scan-Protokoll sind zum Beispiel:

- Archive mit eingeschränktem Zugriff (xar, rar usw.)

  **Lösung**: Finden Sie die Datei über die Option **Im Finder zeigen** und löschen Sie sie von Hand. Vergessen Sie dabei nicht, den Papierkorb zu leeren.

- Postfächer mit eingeschränktem Zugriff (Thunderbird usw.)

  **Lösung**: Entfernen Sie den Eintrag mit der infizierten Datei mithilfe der Anwendung.

- Backup-Inhalte

  **Lösung**: Aktivieren Sie in den Scanner-Einstellungen die Option **Backup-Inhalte nicht scannen** oder schließen Sie die gefundenen Dateien mit **Ausschlüsse hinzufügen** vom Scan aus.

  Werden infizierte Dateien zu einem späteren Zeitpunkt wiederhergestellt, erkennt Bitdefender Antivirus for Mac diese automatisch und leitet geeignete Maßnahmen ein.

> **Beachten Sie**
> Dateien mit beschränktem Zugriff sind Dateien, die Bitdefender Antivirus for Mac zwar öffnen, aber nicht bearbeiten kann.

**Wo kann ich detaillierte Informationen zu den Produktaktivitäten einsehen?**
Bitdefender führt ein Protokoll über alle wichtigen Aktionen, Statusänderungen und andere kritische Nachrichten über die eigenen Aktivitäten. Um auf diese Informationen zuzugreifen, öffnen Sie das Fenster Bitdefender Antivirus for Mac-Einstellungen:

1. Öffnen Sie Bitdefender Antivirus for Mac.
2. Wählen Sie eine der folgenden Methoden:
   - Klicken Sie in der Menüleiste auf Bitdefender Antivirus for Mac und wählen Sie **Präferenzen**.
   - Klicken Sie in der Menüleiste auf das Symbol und wählen Sie **Einstellungen**.
   - Drücken Sie Befehl-Komma (,).
3. Wählen Sie den **Verlauf**-Reiter.

   Details zu den Produktaktivitäten werden angezeigt.

**Kann ich Bitdefender Antivirus for Mac über einen Proxy-Server aktualisieren?**
Bitdefender Antivirus for Mac kann Updates über einen Proxy Server nur dann durchführen, wenn dafür keine Autorisierung notwendig ist. Sie müssen keine Programmeinstellungen konfigurieren.

Wenn Ihre Internetverbindung über einen Proxy-Server läuft, der eine Autorisierung verlangt, müssen Sie regelmäßig zu einer direkten Internetverbindung wechseln, um die neuesten Bedrohungsinformationen herunterladen zu können.

**Wie kann ich Bitdefender Antivirus for Mac entfernen?**
Um Bitdefender Antivirus for Mac zu entfernen, gehen Sie folgendermaßen vor:

1. Öffnen Sie **Finder** und wählen Sie den Programme-Ordner.
2. Öffnen Sie den Bitdefender-Ordner und doppelklicken Sie nach auf Bitdefender-Deinstallationsprogramm.
3. Klicken Sie auf **Deinstallieren**, und warten Sie, bis der Vorgang abgeschlossen ist.
4. Klicken Sie zum Abschluss auf **Schließen**.

**Wichtig**
Ist ein Fehler aufgetreten, so können Sie die Kundenbetreuung von Bitdefender wie in *„Hilfe anfordern“ (S. 341)* beschrieben, kontaktieren.

**Wie entferne ich die Linkchecker-Erweiterungen aus meinem Browser?**

- Um die Linkchecker-Erweiterungen aus Mozilla Firefox zu entfernen, gehen Sie folgendermaßen vor:
  1. Öffnen Sie den Firefox-Browser.
  2. Klicken Sie auf **Tools** und danach auf **Add-ons**.
  3. Klicken Sie in der Spalte links auf **Erweiterungen**.
  4. Wählen Sie die Erweiterung aus und klicken Sie auf **Entfernen**.
  5. Starten Sie den Browser neu, um den Entfernungsvorgang abzuschließen.
- Um die Linkchecker-Erweiterungen aus Google Chrome zu entfernen, gehen Sie folgendermaßen vor:
  1. Öffnen Sie Ihren Chrome-Browser.
  2. Klicken Sie am oberen rechten Bildschirmrand auf **Mehr** .
  3. Wählen Sie im Bereich **Weitere Tools** den Eintrag **Erweiterungen** aus.
  4. Klicken Sie neben der Erweiterung, die Sie entfernen möchten, auf **Aus Chrome entfernen...**
  5. Klicken Sie auf **Entfernen**, um den Entfernungsvorgang zu bestätigen.
- Um Bitdefender TrafficLight aus Safari zu entfernen, gehen Sie folgendermaßen vor:
  1. Öffnen Sie Ihren Safari-Browser.
  2. Klicken Sie in der Browser-Symbolleiste auf und danach auf **Einstellungen**.
  3. Wählen Sie den Reiter **Erweiterungen** aus und suchen Sie in der Liste die Erweiterung **Bitdefender TrafficLight auf Safari**.
  4. Wählen Sie die Erweiterung aus und klicken Sie auf **Deinstallieren**.
  5. Klicken Sie auf **Deinstallieren**, um den Entfernungsvorgang zu bestätigen.

**Wann sollte ich Bitdefender VPN nutzen?**

Bei Aufrufen, Herunterladen oder Hochladen von Inhalten im Internet sollten Sie stets Vorsicht walten lassen. Um sicherzustellen, dass Sie beim Surfen im Netz jederzeit geschützt sind, empfehlen wie den Einsatz von Bitdefender VPN, wenn Sie:

- Verbindungen zu öffentlichen WLAN-Netzwerken herstellen möchten
- auf Inhalte zugreifen möchten, die regionalen Zugangsbeschränkungen unterliegen, egal ob Sie zuhause oder im Ausland sind
- Ihre persönlichen Daten vor Zugriff schützen möchten (Benutzernamen, Passwörter, Kreditkartendaten etc.)
- Ihre IP-Adresse verbergen möchten

**Wirkt sich Bitdefender VPN auf die Akkulaufzeit meines Gerätes aus?**

Bitdefender VPN wurde eigens entwickelt, um Ihre persönlichen Daten zu schützen, Ihre IP-Adresse bei Verbindungen mit ungesicherten WLAN-Netzwerken zu verbergen und Ihnen den Zugriff auf Inhalte mit länderspezifischen Zugangsbeschränkungen zu ermöglichen. Um Ihren Akku zu entlasten, empfehlen wir, das VPN nur bei Bedarf zu nutzen und die Verbindung danach wieder zu trennen.

**Wird meine Internetverbindung langsamer, wenn ich eine Verbindung mit Bitdefender VPN herstelle?**

Bitdefender VPN ist auf einen ressourcenschonenden Betrieb beim Surfen im Netz ausgelegt. Ihre Internetverbindung bzw. die Entfernung zu Server, mit dem Sie eine Verbindung hergestellt haben, können sich jedoch negativ auf die Verbindungsgeschwindigkeit auswirken. Wenn es nicht unbedingt notwendig ist, dass Sie sich von Ihrem Standort aus mit einem weit entfernten Server verbinden (z. B. von Deutschland aus nach China), sollten Sie in solchen Fällen Bitdefender VPN erlauben, automatisch eine Verbindung mit dem nächstgelegenen Server herzustellen bzw. einen Server zu finden, der näher an Ihrem Standort liegt.

# MOBILE SECURITY FÜR IOS

# 14. WORUM HANDELT ES SICH BEI BITDEFENDER MOBILE SECURITY FOR IOS?

Über das Internet kann man schnell und bequem Rechnungen bezahlen, Urlaube buchen sowie Waren und Dienstleistungen erwerben. Die verstärkte Nutzung dieser Online-Dienste geht jedoch auch mit hohen Risiken einher. Ohne die entsprechenden Sicherheitsvorkehrungen können personenbezogene Daten schnell in die falschen Hände gelangen. Was ist also wichtiger, als der Schutz der Daten, die in unseren Online-Konten und Smartphones zu finden sind?

Mit Bitdefender Mobile Security for iOS können Sie:

- Schützen Sie Ihre Daten in ungesicherten WLAN-Netzwerken.
- Überprüfen, ob die Online-Konten, die Sie jeden Tag nutzen, von Datenschutzverletzungen betroffen sind.
- Orten und sperren Sie Ihr Gerät im Falle von Diebstahl oder Verlust und löschen Sie alle gespeicherten Daten.

Bitdefender Mobile Security for iOS wird kostenlos bereitgestellt und muss über ein Bitdefender-Benutzerkonto aktiviert werden.

# 15. ERSTE SCHRITTE

## Systemanforderungen

Bitdefender Mobile Security for iOS eignet sich für iPhones ab iOS 10. Zur Aktivierung und Überprüfung, ob Ihre Online-Konten von Datenschutzverletzungen betroffen sind, wird eine aktive Internetverbindung benötigt.

## Installation von Bitdefender Mobile Security for iOS

- **Über Bitdefender Central**
  - Für iOS
    1. Gehen Sie zu: https://central.bitdefender.com.
    2. Melden Sie sich bei Ihrem Bitdefender-Konto an.
    3. Tippen Sie oben links auf das ☰-Symbol und wählen Sie danach **Meine Geräte** aus.
    4. Tippen Sie **LOKALEN SCHUTZ INSTALLIEREN**.
    5. Wählen Sie Bitdefender Mobile Security aus der Liste und tippen Sie danach auf **ZU APP STORE**.
    6. Tippen Sie im App Store auf **INSTALLIEREN**.
  - Für Windows, macOS, Android
    1. Gehen Sie zu: https://central.bitdefender.com.
    2. Melden Sie sich bei Ihrem Bitdefender-Konto an.
    3. Tippen Sie in der oberen linken Bildschirmecke auf das ☰-Symbol und wählen Sie danach **Meine Geräte** aus.
    4. Tippen Sie **LOKALEN SCHUTZ INSTALLIEREN**.
    5. Klicken Sie auf Windows- und macOS-Geräten auf den Link **Auf einem anderen Gerät**.

       Tippen Sie auf Android-Geräten auf **Möchten Sie weitere Geräte schützen?**.
    6. Wählen Sie **iOS** aus.

7. Wählen Sie **Bitdefender Mobile Security** aus der Liste und tippen Sie danach auf **FORTFAHREN**.
8. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **SENDEN**.
9. Greifen Sie über Ihr iOS-Gerät auf Ihre E-Mails zu und tippen Sie in der von unseren Servern verschickten E-Mail auf **AUS dem AppStore HERUNTERLADEN**.

   Sie werden zur **App Store**-App weitergeleitet.
10. Tippen Sie im App Store auf **INSTALLIEREN**.

- **Über den App Store**

  Suchen Sie nach Bitdefender Mobile Security for iOS, um die App zu finden und zu installieren.

Zum Abschluss des Installationsvorgangs müssen Sie zunächst der Abonnementvereinbarung zustimmen. Bitte nehmen Sie sich einen Moment Zeit, um die Abonnementvereinbarung zu lesen, da Sie hier die Bedingungen finden, unter denen Sie Bitdefender Mobile Security for iOS nutzen dürfen.

Tippen Sie auf **Fortfahren**, um zum nächsten Fenster zu gelangen.

## Melden Sie sich bei Ihrem Bitdefender-Konto an

Zur Verwendung von Bitdefender Mobile Security for iOS müssen Sie Ihr Gerät mit einem Bitdefender-, Facebook-, Google- oder Microsoft-Konto verknüpfen, indem Sie sich über die App bei Ihrem Konto anmelden. Beim ersten Öffnen der App werden Sie zur Anmeldung bei einem Benutzerkonto aufgefordert.

So können Sie Ihr Gerät mit einem Bitdefender-Konto verknüpfen:

1. Geben Sie die E-Mail-Adresse und das Passwort für Ihr Bitdefender-Konto in die entsprechenden Felder ein. Falls Sie noch kein Bitdefender-Konto haben und jetzt eines anlegen möchten, klicken Sie auf den entsprechenden Link.
2. Tippen Sie auf **ANMELDEN**.

Tippen Sie zur Anmeldung mit einem Facebook-, Google- oder Microsoft-Konto im Bereich **ODER MELDEN SIE SICH AN ÜBER** auf den entsprechenden Dienst. Sie werden zur Anmeldeseite des ausgewählten Dienstes weitergeleitet.

Befolgen Sie die Anweisungen zur Verknüpfung Ihres Benutzerkontos mit Bitdefender Mobile Security for iOS.

**Beachten Sie**
Bitdefender hat keinen Zugriff auf Ihre vertraulichen Informationen, so zum Beispiel das Passwort, das Sie zur Anmeldung in Ihrem Konto verwenden, oder die persönlichen Informationen Ihrer Freunde und Kontakte.

## Assistent

Ein Assistent mit Informationen zu den Produktfunktionen wird beim ersten Öffnen der App angezeigt. Wählen Sie **WEITER**, um dem Assistenten weiter zu folgen, oder **Überspringen**, um den Assistenten zu schließen.

## Dashboard

Tippen Sie im App-Depot Ihres Geräts auf das Symbol für Bitdefender Mobile Security for iOS, um die Andwendungsoberfläche anzuzeigen.

Beim ersten Aufrufen der App werden Sie aufgefordert, Ihre Zustimmung zur Übermittlung von Bitdefender-Benachrichtigungen zu erteilen. Tippen Sie auf **Zulassen**, um von Bitdefender über alle relevanten Neuigkeiten zu Ihrer App auf dem Laufenden gehalten zu werden. Sie können die Bitdefender-Benachrichtigungen jederzeit unter Einstellungen > Benachrichtigungen > Mobile Security verwalten.

Tippen Sie unten im Bildschirm auf das entsprechende Symbol, um auf die benötigten Informationen zuzugreifen.

**VPN**
Verschlüsselt die Internetkommunikation und hilft Ihnen so, Ihre Privatsphäre in jedem beliebigen Netzwerk zu schützen. Weitere Informationen finden Sie unter „*VPN*“ (S. 286).

**Kontoschutz**
Erfahren Sie, ob Ihre E-Mail-Konten von Datenschutzverletzungen betroffen sind. Weitere Informationen finden Sie unter „*Kontoschutz*“ (S. 289).

**Diebstahlschutz**
Orten und sperren Sie Ihr Gerät, um zu verhindern, dass Ihre persönlichen Daten in die falschen Hände geraten. Weitere Informationen finden Sie unter „*Diebstahlschutz-Funktionen*“ (S. 291).

Tippen Sie auf das -Symbol Ihres Gerätes, während Sie sich im Hauptmenü der Anwendung befinden, um weitere Optionen anzuzeigen. Die folgenden Optionen werden angezeigt:

- Kaufe wiederherstellen - Hier können Sie das Premium-VPN-Abonnement, das Sie über Ihr iTunes-Konto erworben haben, wiederherstellen.
- Erste Schritte - Hiermit starten Sie eine kurze Einführung in das Produkt.
- Feedback - Hiermit starten Sie Ihre Standard-E-Mail-Anwendung, über die Sie uns Ihre Meinung zur App zukommen lassen können.
- App-Info - Hiermit rufen Sie Informationen zur installierten Version sowie die Abonnementvereinbarung, Datenschutzrichtlinie und Informationen zur Einhaltung der Bedingungen von Open-Source-Lizenzen ein.

# 16. VPN

Mit Bitdefender VPN schützen Sie Ihre Daten bei Verbindungen mit ungesicherten WLAN-Netzwerken wie zum Beispiel in Flughäfen, Einkaufszentren, Cafés oder Hotels. So vermeiden Sie unglückliche Situationen wie den Diebstahl Ihrer persönlichen Daten oder Versuche, Ihre Geräte-IP-Adresse für Hacker offenzulegen.

Das VPN dient als Tunnel zwischen Ihrem Gerät und dem Netzwerk, mit dem Sie sich verbinden. Ihre Verbindung wird abgesichert, Ihren Daten werden professionell nach Bankenstandard verschlüsselt und Ihre IP-Adresse bleibt jederzeit unsichtbar. Ihr Datenverkehr wird über spezielle Server weitergeleitet, was es nahezu unmöglich macht, Ihr Gerät neben den unzähligen anderen Geräten zu identifizieren, die ebenfalls unsere Dienste in Anspruch nehmen. Darüber hinaus können Sie mit Bitdefender VPN im Internet auch auf solche Inhalte zugreifen, die üblicherweise regionalen Zugangsbeschränkungen unterliegen.

### Beachten Sie

In manchen Ländern wird Internetzensur betrieben. Aus diesem Grund ist die Nutzung von VPNs hier gesetzlich verboten. Um rechtliche Folgen vorzubeugen, kann es sein, dass eine Warnmeldung angezeigt wird, wenn Sie zum ersten Mal versuchen, die VPN-Funktion von Bitdefender zu verwenden. Wenn Sie die Funktion dann verwenden, bestätigen Sie damit, dass Sie die relevanten Bestimmungen Ihres Landes kennen und sich der entsprechenden Risiken bewusst sind

So aktivieren Sie Bitdefender VPN:

1. Tippen Sie unten auf dem Bildschirm auf das -Symbol.
2. Tippen Sie auf **Verbinden**, um sich und Ihre Geräte bei Verbindungen mit ungesicherten WLAN-Netzwerken zu schützen.

   Tippen Sie auf **Trennen**, um die Verbindung wieder aufzuheben.

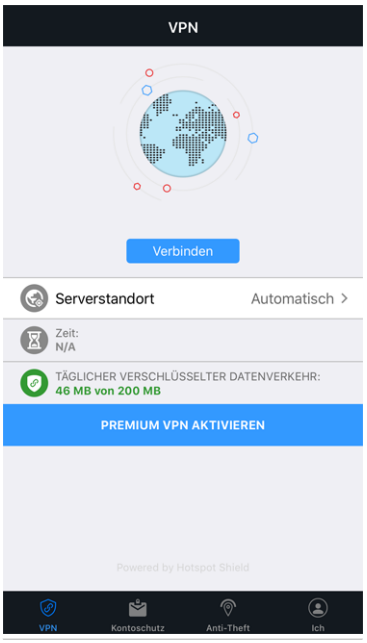
### Beachten Sie

Beim ersten Aktivieren des VPNs werden Sie aufgefordert, Bitdefender die Erlaubnis zur Einrichtung der VPN-Konfiguration zur Überwachung Ihres Netzwerkdatenverkehrs zu erteilen. Tippen Sie zum Fortfahren auf **Zulassen**. Wenn Sie zum Schutz Ihres Smartphones eine Authentifizierungsmethode (Fingerabdruck oder PIN) festgelegt haben, wird diese jetzt abgefragt.

Das VPN Symbol wird bei aktivem VPN in der Statusleiste angezeigt.

Um Ihren Akku zu schonen, empfehlen wir Ihnen, VPN zu deaktivieren, wenn Sie es nicht mehr benötigen.

Falls Sie über ein Premium-Abonnement verfügen und sich mit einem Server Ihrer Wahl verbinden möchten, tippen Sie in der VPN-Benutzeroberfläche auf **Serverstandort** und wählen Sie den gewünschten Standort aus. Weitere Einzelheiten zu den VPN-Abonnments finden Sie unter *„Abonnements“ (S. 287)*.




VPN

## 16.1. Abonnements

Mit Bitdefender VPN erhalten Sie ein kostenloses Datenvolumen von 200 MB pro Tag, um Ihre Verbindung bei Bedarf abzusichern. Sie werden automatisch mit dem besten Serverstandort verbunden.

Wenn Sie sich für ein Upgrade auf die Premium-Version entscheiden, entfällt das Datenlimit und Sie können durch die freie Wahl des Serverstandorts Inhaltsbeschränkungen überall auf der Welt umgehen.

Sie können jederzeit ein Upgrade auf Bitdefender Premium VPN vornehmen, indem Sie in der VPN-Benutzeroberfläche auf **PREMIUM VPN AKTIVIEREN** tippen.

Ein Bitdefender Premium-VPN-Abonnement läuft unabhängig von dem kostenlosen Bitdefender Mobile Security for iOS-Abonnement, d. h. Sie können es über den gesamten Verfügbarkeitszeitraum hinweg nutzen. Bei Ablauf des Bitdefender Premium-VPN-Abonnement kehren Sie automatisch zum kostenlosen Angebot zurück.

Bitdefender VPN ist ein plattformübergreifendes Produkt, das in Bitdefender-Produkten für Windows, macOS, Android und iOS verfügbar ist. Nach einem Premium-Upgrade können Sie Ihr Abonnement in allen Produkten nutzen, vorausgesetzt, dass Sie sich mit dem gleichen Bitdefender-Benutzerkonto anmelden.

# 17. KONTOSCHUTZ

Der Bitdefender-Kontoschutz erkennt, ob die Datensicherheit der Benutzerkonten kompromittiert wurde, über die Sie Ihre Online-Zahlungen und -Einkäufe abwickeln und sich bei Ihren Apps oder Websites anmelden. Die unter Ihren Konten gespeicherten Daten umfassen Passwörter, Kreditkartendaten und Bankinformationen. Wurden diese nicht ausreichend abgesichert, kann es zu Identitätsdiebstahl und Verletzungen Ihrer Privatsphäre kommen.

Nach der Bestätigung wird der Privatsphärestatus des Benutzerkontos umgehend angezeigt.

Tippen Sie auf **Auf Datenlecks prüfen**, um zu prüfen, ob Ihre Benutzerkonten von Datenschutzverletzungen betroffen sind.

So können Sie Ihre persönlichen Daten schützen:

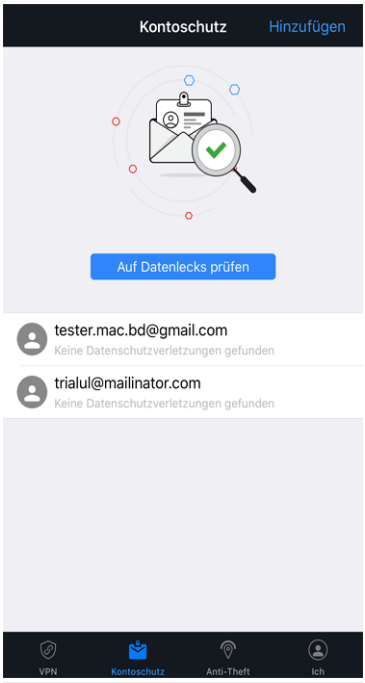
1. Tippen Sie unten auf dem Bildschirm auf das -Symbol.
2. Tippen Sie oben rechts auf dem Bildschirm auf **Hinzufügen**.
3. Geben Sie Ihre E-Mail-Adresse in das entsprechende Feld ein und tippen Sie danach auf **Weiter**.

   Bitdefender muss für dieses Konto vor der Preisgabe privater Daten erst eine Kontovalidierung durchführen. Sie erhalten zu diesem Zweck unter der angegebenen E-Mail-Adresse einen Bestätigungscode.
4. Rufen Sie Ihre E-Mails ab und geben Sie den erhaltenen Code in Ihrer App im Bereich **Kontoschutz** ein. Falls Sie Bestätigungs-E-Mail in Ihrem Posteingang nicht finden können, überprüfen Sie bitte Ihren Spam-Ordner.

   Der Privatsphärestatus des bestätigten Kontos wird angezeigt.

Wurden Datenschutzverletzungen bei einem Ihrer Benutzerkonten festgestellt, empfehlen wir Ihnen, so schnell wie möglich das entsprechende Passwort zu ändern. Mit diesen Tipps sorgen Sie für sichere Passwörter:

- Verwenden Sie mindestens acht Zeichen.
- Verwenden Sie Groß- und Kleinbuchstaben.
- Verwendenden Sie mindestens eine Zahl oder Sonderzeichen wie #, @, % oder !.




Kontoschutz

# 18. DIEBSTAHLSCHUTZ-FUNKTIONEN

Bitdefender kann Ihnen dabei helfen, Ihr Gerät zu finden, und verhindert, dass Ihre privaten Daten in die falschen Hände gelangen.

Sie müssen nur den Diebstahlschutz über das Gerät aktivieren und können dann bei Bedarf jederzeit und mit jedem Browser auf **Bitdefender Central** zugreifen.

Bitdefender Mobile Security for iOS bietet die folgenden Diebstahlschutzfunktionen:

**Fern-Gerätortung**
Hiermit können Sie den Standort Ihres Geräts in Maps anzeigen.

Die Genauigkeit der Ortung hängt davon ab, wie gut Bitdefender seinen Standort bestimmen kann:

- Wenn GPS im Gerät aktiviert ist, kann sein Standort bis auf ein paar Meter genau bestimmt werden, solange das Gerät in Reichweite der GPS-Satelliten (d. h. nicht in einem Gebäude) ist.
- Wenn sich das Gerät in einem Gebäude befindet, kann sein Standort auf mehrere zehn Meter genau bestimmt werden, solange WLAN aktiviert ist und Drahtlosnetzwerke in Reichweite des Geräts sind.
- Andernfalls wird der Standort allein über Daten aus dem Mobilfunknetzwerk bestimmt, wodurch die Genauigkeit auf einen Umkreis von ein paar hundert Metern sinkt.

**Fernsperrung**
Sperren Sie Ihren Gerätebildschirm per Fernzugriff.

**Fernlöschung**
Löschen Sie alle persönlichen Daten von Ihrem Gerät.

## Aktivierung des Diebstahlschutzes

Gehen Sie folgendermaßen vor, um die Diebstahlschutzfunktionen zuaktivieren:

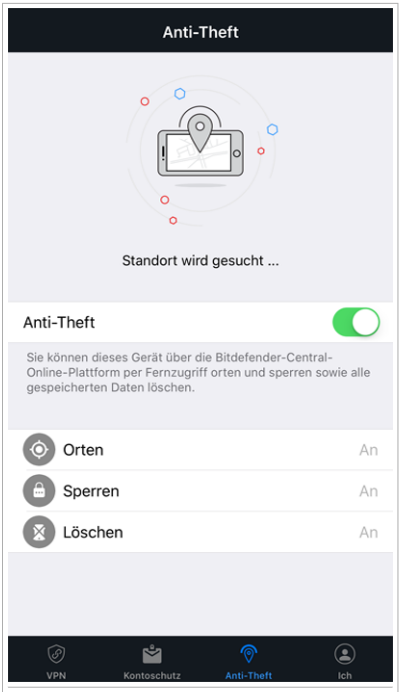
1. Tippen Sie unten auf dem Bildschirm auf das -Symbol.
2. Aktivieren Sie den Schalter.

3. Erlauben Sie den Zugriff auf den Gerätestandort, damit Bitdefender Ihr Gerät im Falle von Diebstahl oder Verlust orten kann. Diese Benachrichtigung wird bei der ersten Aktivierung des Bitdefender-Diebstahlschutzes angezeigt. Sie können den Bitdefender-Zugriff jederzeit unter Einstellungen > Datenschutz > Lokalisierungsdienste > Mobile Security verwalten.
4. Wenn Sie die Diebstahlschutzfunktion auf Ihrem Gerät zum ersten Mal aktivieren, werden Sie zudem aufgefordert, ein MDM-Profil (Mobile Device Management) zu installieren. Gehen Sie dabei folgendermaßen vor:
   a. Tippen Sie auf **Zulassen**, um zu den Einstellungen zu gelangen.
   b. Tippen Sie auf **Zulassen**, um das MDM-Profil (Mobile Device Management) zu installieren, das von Bitdefender zum Abschluss des Aktivierungsprozesses benötigt wird.

      Wurde zum Schutz Ihres Smartphones eine PIN festgelegt, wird diese jetzt abgefragt.
   c. Lesen Sie die Informationen zum CA-Root-Zertifikat und Mobile Device Management.
   d. Wenn Sie den Bedingungen zustimmen, tippen Sie auf **Installieren**.
   e. Tippen Sie im Fenster Fernverwaltung auf **Anerkennen** und danach auf **Fertig**, um das Fenster wieder zu schließen.

### Beachten Sie

Sollte die Installation des aktuellen Bitdefender-MDM-Profils fehlschlagen, muss unter Umständen ein altes, bereits installiertes MDM-Profil entfernt werden. Gehen Sie zu Einstellungen > Allgemein > Geräteverwaltung > Bitdefender. Wählen Sie das erkannte Profil aus und tippen Sie auf **Verwaltung entfernen**. Wurde zum Schutz Ihres Smartphones eine PIN festgelegt, wird diese jetzt abgefragt. Tippen Sie anschließend erneut auf **Verwaltung entfernen**, um Ihre Auswahl zu bestätigen. Versuchen Sie erneut, den Diebstahlschutz zu aktivieren. Sollte das Problem weiter bestehen, wenden Sie sich bitte per E-Mail an unser Team unter bdios@bitdefender.com.




Diebstahlschutz

# Nutzung der Diebstahlschutzfunktionen über Bitdefender Central (Web-Steuerung)

So können Sie über Ihr Bitdefender-Konto auf die Diebstahlschutzfunktionen zugreifen:

1. Gehen Sie zu: https://central.bitdefender.com.
2. Melden Sie sich bei Ihrem Bitdefender-Konto an.
3. Tippen Sie oben links auf das ☰-Symbol und wählen Sie danach **Meine Geräte** aus.
4. Tippen Sie auf die gewünschte Gerätekarte und wechseln Sie danach zum Reiter **Diebstahlschutz**.
5. Tippen Sie in dem Feld unten im Fenster auf das Symbol für die Funktion, die Sie nutzen möchten:

**IP ANZEIGEN** - Zeigt die letzte IP-Adresse für das ausgewählte Gerät an.
**Orten** - Zeigt den Standort Ihres Geräts auf Maps an.
**Verriegeln** - den Computer verriegeln und eine PIN zur Entriegelung festlegen.
**Löschen** - Entfernen aller Daten auf Ihrem Gerät.

### Wichtig
Nach einer Löschung funktionieren die Diebstahlschutz-Funktionen nicht mehr.

# 19. BITDEFENDER BENUTZERKONTO

Zur Aktivierung von Bitdefender Mobile Security for iOS ist ein Bitdefender-Benutzerkonto zwingend erforderlich. Sie können sich jederzeit über jeden beliebigen Computer und jedes internetfähige Gerät unter https://central.bitdefender.com bei Ihrem Benutzerkonto anmelden, um auf die Online-Funktionen und -Dienste zuzugreifen oder per Fernzugriff wichtige Aktionen auf den Geräten auszuführen, auf denen Bitdefender installiert ist.

## Meine Geräte

Über Ihr Bitdefender-Benutzerkonto können Sie im Bereich **Meine Geräte** die Bitdefender-Produkte auf Ihren Geräten aus der Ferne installieren und verwalten, sofern die Geräte eingeschaltet und mit dem Internet verbunden sind. Auf den Gerätekacheln sind der Gerätename, der Sicherheitsstatus angegeben sowie die Information, ob Sicherheitsprobleme auf Ihren Geräten bestehen.

Um Ihre Geräte bequem zuordnen und verwalten zu können, können Sie den Gerätenamen selbst festlegen und für jedes Gerät einen Besitzer anlegen bzw. zuweisen:

1. Tippen Sie oben links auf das ☰-Symbol und wählen Sie danach **Meine Geräte** aus.
2. Tippen Sie auf die gewünschte Gerätekachel und dann auf das Symbol ⋮ in der rechten oberen Ecke. Die folgenden Optionen sind verfügbar:

- **Einstellungen** - Hier können Sie den Namen des ausgewählten Gerätes ändern.
- **Profil** - Hier können Sie dem ausgewählten Gerät ein Profil zuordnen. Tippen Sie auf **Besitzer hinzufügen**, füllen Sie die entsprechenden Felder aus, geben Sie Namen, E-Mail-Adresse, Telefonnummer und Geburtsdatum ein und fügen Sie bei Bedarf ein Profilbild hinzu.
- **Entfernen** - Hier können Sie ein Profil und das dem Profil zugewiesene Gerät aus Ihrem Bitdefender-Benutzerkonto entfernen.

## Anmelden mit einem anderen Bitdefender-Konto

Gehen Sie folgendermaßen vor, um sich mit einem anderen Bitdefender-Konto anzumelden:

1. Tippen Sie unten auf dem Bildschirm auf das -Symbol.
2. Tippen Sie oben rechts auf dem Bildschirm auf das -Symbol.
3. Tippen Sie auf **Abmelden**.
4. Geben Sie die E-Mail-Adresse und das Passwort für Ihr Bitdefender-Konto in die entsprechenden Felder ein.
5. Tippen Sie auf **ANMELDEN**.

# MOBILE SECURITY FÜR ANDROID

# 20. SICHERHEITSFUNKTIONEN

Bitdefender Mobile Security schützt Ihr Android-Gerät mit den folgenden Funktionen:

- Virenscanner
- Kontoschutz
- Internet-Schutz
- VPN
- Diebstahlschutz:
  - Fern-Gerätortung
  - Fern-Gerätesperrung
  - Fern-Gerätelöschung
  - Fern-Tonsignale
- App-Sperre
- Berichte
- WearON

Sie können die Produktfunktionen 14 Tage lange kostenlos verwenden. Nach Ablauf dieses Zeitraums müssen Sie die Vollversion erwerben, um Ihr Mobilgerät zu schützen.

# 21. ERSTE SCHRITTE

## Systemanforderungen

Bitdefender Mobile Security läuft auf allen Geräten ab Android 4.0.3. Für den Bedrohungs-Scan über die Cloud wird eine aktive Internet-Verbindung benötigt.

## Installation von Bitdefender Mobile Security

- **Über Bitdefender Central**
  - Android
    1. Gehen Sie zu: https://central.bitdefender.com.
    2. Melden Sie sich bei Ihrem Bitdefender-Konto an.
    3. Tippen Sie oben links auf das ☰-Symbol und wählen Sie danach **Meine Geräte** aus.
    4. Tippen Sie **LOKALEN SCHUTZ INSTALLIEREN**.
    5. Wählen Sie **Bitdefender Mobile Security** aus der Liste und tippen Sie danach auf **ZU GOOGLE PLAY**.
    6. Tippen Sie im Google-Play-Fenster auf **INSTALLIEREN**.
  - Auf Windows, macOS, iOS
    1. Gehen Sie zu: https://central.bitdefender.com.
    2. Melden Sie sich bei Ihrem Bitdefender-Konto an.
    3. Tippen Sie in der oberen linken Bildschirmecke auf das ☰-Symbol und wählen Sie danach **Meine Geräte** aus.
    4. Tippen Sie **LOKALEN SCHUTZ INSTALLIEREN**.
    5. Klicken Sie auf Windows- und macOS-Geräten auf den Link **Auf einem anderen Gerät**.

       Tippen Sie auf iOS-Geräten auf **Möchten Sie weitere Geräte schützen?**.
    6. Wählen Sie **Android** aus.
    7. Wählen Sie **Bitdefender Mobile Security** aus der Liste und tippen Sie danach auf **FORTFAHREN**.

8. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und tippen Sie dann auf **SENDEN**.
9. Greifen Sie über Ihr Android-Gerät auf Ihr E-Mail-Konto zu und tippen Sie auf **Jetzt über Google Play herunterladen**.

   Sie werden zur **Google Play**-App weitergeleitet.
10. Tippen Sie im Google-Play-Fenster auf **INSTALLIEREN**.

- **Über Google Play**

  Suchen Sie nach Bitdefender Mobile Security, um die App zu finden und zu installieren.

  Sie können auch den QR-Code einscannen:

QR-Code

Zum Abschluss des Installationsvorgangs müssen Sie zunächst der Abonnementvereinbarung zustimmen. Bitte nehmen Sie sich einen Moment Zeit, um die Abonnementvereinbarung zu lesen, da Sie hier die Bedingungen finden, unter denen Sie Bitdefender Mobile Security nutzen dürfen.

Tippen Sie auf **Fortfahren**, um zum nächsten Fenster zu gelangen.

## Melden Sie sich bei Ihrem Bitdefender-Konto an

Zur Verwendung von Bitdefender Mobile Security müssen Sie Ihr Gerät mit einem Bitdefender-, Facebook-, Google- oder Microsoft-Konto verknüpfen, indem Sie sich über die App bei Ihrem Konto anmelden. Beim ersten Öffnen der App werden Sie zur Anmeldung bei einem Benutzerkonto aufgefordert.

Wenn Sie Bitdefender Mobile Security über Ihr Bitdefender-Konto installiert haben, wird die App automatisch versuchen, sich bei diesem Konto anzumelden.

So können Sie Ihr Gerät mit einem Bitdefender-Konto verknüpfen:

1. Öffnen Sie Bitdefender Mobile Security.
2. Geben Sie die E-Mail-Adresse und das Passwort für Ihr Bitdefender-Konto in die entsprechenden Felder ein. Falls Sie noch kein Bitdefender-Konto haben und jetzt eines anlegen möchten, klicken Sie auf den entsprechenden Link.
3. Tippen Sie auf **ANMELDEN**.

Tippen Sie zur Anmeldung mit einem Facebook-, Google- oder Microsoft-Konto im Bereich **ODER MELDEN SIE SICH AN ÜBER** auf den entsprechenden Dienst. Sie werden zur Anmeldeseite des ausgewählten Dienstes weitergeleitet. Befolgen Sie die Anweisungen zur Verknüpfung Ihres Benutzerkontos mit Bitdefender Mobile Security.

**Beachten Sie**
Bitdefender hat keinen Zugriff auf Ihre vertraulichen Informationen, so zum Beispiel das Passwort, das Sie zur Anmeldung in Ihrem Konto verwenden, oder die persönlichen Informationen Ihrer Freunde und Kontakte.

## Aktivierung von Bitdefender Mobile Security

Um mit Bitdefender Mobile Security umfassend geschützt zu sein, müssen Sie Ihr Produkt zunächst mit einem Abonnement aktivieren. Dieses legt fest, wie lange Sie das Produkt nutzen können. Nach Ablauf des Abonnements wird die Anwendung nicht mehr funktionieren und Ihr Gerät nicht mehr schützen.

So können Sie Bitdefender Mobile Security aktivieren:

1. Öffnen Sie Bitdefender Mobile Security.
2. Die Anwendung zeigt Informationen zum aktuellen Abonnementstatus an.

   Tippen Sie auf **ICH HABE EINEN CODE**.
3. Geben Sie einen Aktivierungscode in das entsprechende Feld ein und tippen Sie danach auf **AKTIVIEREN**.

So können Sie ein verfügbares Abonnement verlängern:

1. Öffnen Sie Bitdefender Mobile Security.
2. Tippen Sie auf **Menü** und wählen Sie **Mein Konto** aus der Liste aus.

3. Geben Sie unter **Abonnement verlängern** einen Aktivierungscode ein und tippen Sie danach auf **AKTIVIEREN**.

   Alternativ können Sie Ihr aktuelles Abonnement auch über die aufgeführten Angebote verlängern.

# Dashboard

Tippen Sie im App-Depot Ihres Geräts auf das Symbol für Bitdefender Mobile Security, um die Andwendungsoberfläche anzuzeigen.

Das Dashboard zeigt Informationen zum Sicherheitsstatus Ihres Geräts an und lässt Sie komfortabel sämtliche Sicherheitsfunktionen verwalten.

Wenn ein Prozess ausgeführt wird oder eine Funktion Ihre Aufmerksamkeit erfordert, wird eine Kachel mit weiteren Informationen und möglichen Aktionen im Dashboard angezeigt.

Sie können auf die Bitdefender Mobile Security-Funktionen zugreifen und über die **Menu**-Schaltfläche oben links im Fenster bequem zwischen den einzelnen Bereichen wechseln:

**Virenscanner**
Hiermit können Sie Bedarf-Scans starten oder Speicher-Scans aktivieren und deaktivieren. Weitere Informationen finden Sie unter *„Virenscanner“ (S. 304)*.

**Kontoschutz**
Prüft, ob die Datensicherheit Ihrer Online-Konten kompromittiert wurde. Weitere Informationen finden Sie unter *„Kontoschutz“ (S. 307)*.

**Internet-Schutz**
Hiermit können Sie den Internet-Schutz aktivieren und deaktivieren. Weitere Informationen finden Sie unter *„Internet-Schutz“ (S. 309)*.

**VPN**
Verschlüsselt die Internetkommunikation und hilft Ihnen so, Ihre Privatsphäre in jedem beliebigen Netzwerk zu schützen. Weitere Informationen finden Sie unter *„VPN“ (S. 311)*.

**Diebstahlschutz**
Hiermit können Sie die Diebstahlschutzfunktionen aktivieren und deaktivieren und die Einstellungen für den Diebstahlschutz konfigurieren. Weitere Informationen finden Sie unter *„Diebstahlschutz-Funktionen“ (S. 315)*.

**App-Sperre**

Hiermit können Sie Ihre installierten Anwendungen durch Festlegung einer PIN für den Zugriff schützen. Weitere Informationen finden Sie unter „*App-Sperre*“ (S. 321).

**Berichte**

Führt ein Protokoll über alle wichtigen Aktionen, Statusänderungen und andere kritische Nachrichten im Zusammenhang mit den Aktivitäten Ihres Geräts. Weitere Informationen finden Sie unter „*Berichte*“ (S. 326).

**WearON**

Kommuniziert mit Ihrer Smartwatch, damit Sie Ihr Telefon schneller wiederfinden können. Weitere Informationen finden Sie unter „*WearON*“ (S. 327).

# 22. VIRENSCANNER

Bitdefender schützt Ihr Gerät und Ihre Daten mit Scans während der Installation und bei Bedarf vor schädlichen Anwendungen.

**Beachten Sie**
Stellen Sie sicher, dass Ihr Mobilgerät mit dem Internet verbunden ist. Sollte keine Internet-Verbindung bestehen, wird der Scan-Vorgang nicht gestartet.

- **Installations-Scans**

  Jedes Mal, wenn Sie eine Anwendung installieren, scannt Bitdefender Mobile Security sie automatisch über die Cloud-Technologie. Der gleiche Scan-Vorgang wird bei jedem Update einer installierten App wiederholt.

  Dieser Scan-Typ wird über die Autopilot-Funktion bereitgestellt. Der Autopilot ist ein intelligenter Scanner, der alle Apps überprüft, die Sie installieren oder aktualisieren, und so Bedrohungen rechtzeitig aufhält.

  Wenn die Anwendung als schädlich eingestuft wird, wird eine Aufforderung angezeigt, die Anwendung zu deinstallieren. Tippen Sie auf **Deinstallieren**, um zum Deinstallationsbildschirm der Anwendung zu gelangen.

- **Bedarf-Scan**

  Wenn Sie einmal unsicher sein sollten, ob eine Anwendung auf Ihrem Gerät sicher ist, können Sie einen Bedarf-Scan starten.

  Tippen Sie zum Durchführen eines Bedarf-Scans in der Virenscanner-Kachel im Dashboard auf **SCAN STARTEN**.

  Alternativ können Sie einen Scan folgendermaßen durchführen:

  1. Öffnen Sie Bitdefender Mobile Security.
  2. Tippen Sie auf **Menü** und wählen Sie **Virenscanner** aus der Liste aus.
  3. Tippen Sie auf **SCAN STARTEN**.

  **Beachten Sie**
  Für den Virenscanner werden unter Android 6 zusätzliche Berechtigungen benötigt. Tippen Sie auf **SCAN STARTEN** und wählen Sie danach **Zulassen** für folgende Anfragen aus:

  - Zulassen, dass der **Virenschutz** Anrufe tätigt und verwaltet?

- Zulassen, dass der **Virenschutz** auf Fotos, Medien und Dateien auf Ihrem Gerät zugreift?

Der Scanvorgang wird angezeigt. Sie können ihn jederzeit abbrechen.

Malware-Scan

Bitdefender Mobile Security scannt standardmäßig den internen Speicher Ihres Gerätes sowie vorhandene SD-Karten. So können gefährliche Anwendungen, die sich auf der Karte befinden könnten, erkannt werden, bevor Sie Schaden anrichten können.

So aktivieren oder deaktivieren Sie die Option Speicher prüfen:

1. Öffnen Sie Bitdefender Mobile Security.
2. Tippen Sie auf **Menü** und wählen Sie **Virenscanner** aus der Liste aus.

3. Tippen Sie auf den entsprechenden Schalter.

Sie können den Speicher-Scan auch über die **Einstellungen** aktivieren oder deaktivieren. Tippen Sie dazu zunächst auf die -Schaltfläche und danach auf den entsprechenden Schalter.

Wird eine schädliche Anwendung gefunden, werden entsprechende Informationen zu dieser Anwendung angezeigt. Tippen Sie auf **DEINSTALLIEREN**, um sie zu entfernen.

Die Virenscanner-Kachel zeigt den Status Ihres Geräts an. Ein grüne Kachel zeigt, dass Ihr Gerät geschützt ist. Ein rote Kachel bedeutet, dass ein Scan durchgeführt werden muss oder Ihre Aufmerksamkeit gefordert ist.

# 23. KONTOSCHUTZ

Der Bitdefender-Kontoschutz erkennt, ob die Datensicherheit der Benutzerkonten kompromittiert wurde, über die Sie Ihre Online-Zahlungen und -Einkäufe abwickeln und sich bei Ihren Apps oder Websites anmelden. Die unter Ihren Konten gespeicherten Daten umfassen Passwörter, Kreditkartendaten und Bankinformationen. Wurden diese nicht ausreichend abgesichert, kann es zu Identitätsdiebstahl und Verletzungen Ihrer Privatsphäre kommen.

Nach der Bestätigung wird der Privatsphärestatus des Benutzerkontos umgehend angezeigt.

Im Hintergrund werden automatisch weitere Prüfungen durchgeführt und Sie können darüber hinaus täglich manuelle Prüfungen durchführen.

Sie erhalten eine Benachrichtigung, sobald neue Sicherheitsverletzungen bekannt werden, die eines Ihrer bestätigten E-Mail-Konten betreffen.

So können Sie Ihre persönlichen Daten schützen:

1. Öffnen Sie Bitdefender Mobile Security.
2. Tippen Sie auf **Menü** und wählen Sie **Kontoschutz** aus der Liste aus.
3. Tippen Sie auf den blauen Kreis unten rechts auf dem Bildschirm.
4. Geben Sie Ihre E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **WEITER**.

   Bitdefender muss für dieses Konto vor der Preisgabe privater Daten erst eine Kontovalidierung durchführen. Sie erhalten zu diesem Zweck unter der angegebenen E-Mail-Adresse einen Bestätigungscode.
5. Rufen Sie Ihre E-Mails ab und geben Sie den erhaltenen Code in Ihrer App im Bereich **Kontoschutz** ein. Falls Sie Bestätigungs-E-Mail in Ihrem Posteingang nicht finden können, überprüfen Sie bitte Ihren Spam-Ordner.

   Der Privatsphärestatus des bestätigten Kontos wird angezeigt.

Wurden Datenschutzverletzungen bei einem Ihrer Benutzerkonten festgestellt, empfehlen wir Ihnen, so schnell wie möglich das entsprechende Passwort zu ändern. Mit diesen Tipps sorgen Sie für sichere Passwörter:

- Verwenden Sie mindestens acht Zeichen.
- Verwenden Sie Groß- und Kleinbuchstaben.

- Verwendenden Sie mindestens eine Zahl oder Sonderzeichen wie #, @, % oder !.

Nachdem Sie ein Konto gesichert haben, das von einer Datenpanne betroffen war, können Sie die Änderungen bestätigen, indem Sie die identifizierten Datenpannen als **Gelöst** markieren. Dazu müssen Sie:

1. Öffnen Sie Bitdefender Mobile Security.
2. Tippen Sie auf **Menü** und wählen Sie **Kontoschutz** aus der Liste aus.
3. Tippen Sie auf das Konto, das Sie gerade gesichert haben.
4. Streichen Sie im Bereich **Datenpannen** nach links über die Datenpanne, für die Sie das Konto gesichert haben.
5. Tippen Sie auf das Symbol .
6. Die Karte **Als gelöst markieren** wird angezeigt.

   Tippen Sie auf **BESTÄTIGEN**, um zu bestätigen, dass das Konto gesichert wurde.

Wenn alle gefundenen Datenpannen als **Gelöst** markiert wurden, wird das Konto nicht mehr als von einer Datenpanne betroffen angezeigt, zumindest bis es zu einer weiteren Datenpanne kommt.

# 24. INTERNET-SCHUTZ

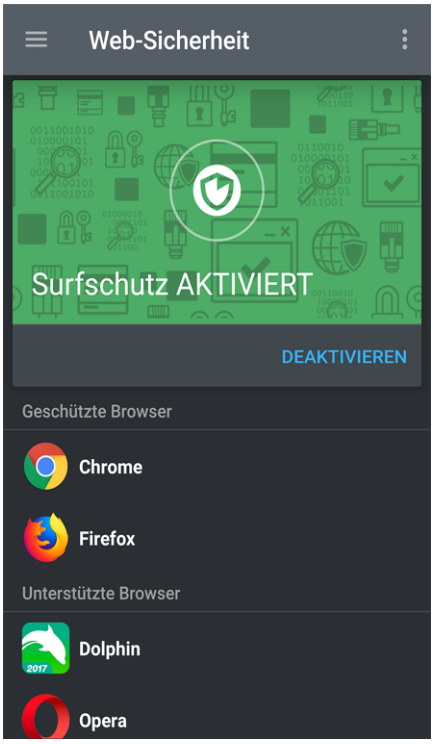
Der Surfschutz nutzt die Bitdefender-Cloud-Dienste, um die von Ihnen im Standard-Android-Browser, in Google Chrome, Firefox, Opera, Opera Mini und Dolphin. Im Bereich Surfschutz finden Sie eine Liste mit allen unterstützten Browsern.

Wenn eine URL auf eine bekannte Phishingversuche oder andere Arten von Betrug oder auf schädliche Inhalte wie Spyware oder Viren, wird die Webseite vorübergehend blockiert und eine Warnung angezeigt.

Sie können dann die Benachrichtigung ignorieren und die Webseite besuchen oder zu einer sicheren Seite zurückkehren.

## Beachten Sie

Für den Surfschutz werden unter Android 6 zusätzliche Berechtigungen benötigt.
Erteilen Sie die Erlaubnis zur Registrierung als Accessibility-Dienst und tippen Sie nach Aufforderung auf **AKTIVIEREN**. Tippen Sie auf **Antivirus** und aktivieren Sie den Schalter. Bestätigen Sie anschließend, dass Sie dem Zugriff auf die Berechtigungen Ihre Geräts zustimmen.




Internet-Schutz

# 25. VPN

Mit Bitdefender VPN schützen Sie Ihre Daten bei Verbindungen mit ungesicherten WLAN-Netzwerken wie zum Beispiel in Flughäfen, Einkaufszentren, Cafés oder Hotels. So vermeiden Sie unglückliche Situationen wie den Diebstahl Ihrer persönlichen Daten oder Versuche, Ihre Geräte-IP-Adresse für Hacker offenzulegen.

Das VPN dient als Tunnel zwischen Ihrem Gerät und dem Netzwerk, mit dem Sie sich verbinden. Ihre Verbindung wird abgesichert, Ihren Daten werden professionell nach Bankenstandard verschlüsselt und Ihre IP-Adresse bleibt jederzeit unsichtbar. Ihr Datenverkehr wird über spezielle Server weitergeleitet, was es nahezu unmöglich macht, Ihr Gerät neben den unzähligen anderen Geräten zu identifizieren, die ebenfalls unsere Dienste in Anspruch nehmen. Darüber hinaus können Sie mit Bitdefender VPN im Internet auch auf solche Inhalte zugreifen, die üblicherweise regionalen Zugangsbeschränkungen unterliegen.

### Beachten Sie

In manchen Ländern wird Internetzensur betrieben. Aus diesem Grund ist die Nutzung von VPNs hier gesetzlich verboten. Um rechtliche Folgen vorzubeugen, kann es sein, dass eine Warnmeldung angezeigt wird, wenn Sie zum ersten Mal versuchen, die VPN-Funktion von Bitdefender zu verwenden. Wenn Sie die Funktion dann verwenden, bestätigen Sie damit, dass Sie die relevanten Bestimmungen Ihres Landes kennen und sich der entsprechenden Risiken bewusst sind.

Sie haben zwei Optionen zur Aktivierung oder Deaktivierung von Bitdefender VPN:

- Tippen Sie in der VPN-Kachel im Dashboard auf die Ein/Aus-Schaltfläche.

  Der Status von Bitdefender VPN wird angezeigt.

- Tippen Sie auf **Menü** und wählen Sie **VPN** aus der Liste aus.

  Tippen Sie auf **Verbinden**, um sich und Ihre Geräte bei Verbindungen mit ungesicherten WLAN-Netzwerken zu schützen.

  Tippen Sie auf **Trennen**, um die Verbindung wieder aufzuheben.

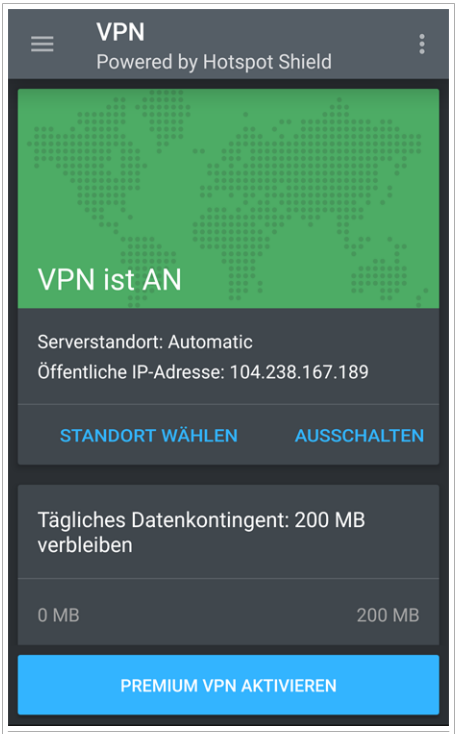
### Beachten Sie

Wenn Sie VPN das erste Mal einschalten, werden Sie gebeten, Bitdefender zu erlauben, eine VPN-Verbindung herzustellen, die den Netzwerkdatenverkehr überwacht. Tippen Sie auf **OK** um fortzufahren.

Das Symbol wird bei aktivem Bitdefender VPN in der Statusleiste angezeigt.

Um Ihren Akku zu schonen, empfehlen wir Ihnen, die VPN-Funktion zu deaktivieren, wenn Sie sie nicht mehr benötigen.

Falls Sie über ein Premium-Abonnement verfügen und sich mit einem Server Ihrer Wahl verbinden möchten, tippen Sie in der VPN-Funktion auf **STANDORT WÄHLEN** und wählen Sie den gewünschten Standort aus. Weitere Einzelheiten zu den VPN-Abonnments finden Sie unter „Abonnements“ (S. 313).




VPN

Tippen Sie in der VPN-Kachel im Dashboard auf **WEITERE INFORMATIONEN**, um auf die Funktion zuzugreifen. Hier können Sie:

- Anzeigen, wie viel von Ihrem täglichen Datenvolumen Sie bereits verbraucht haben, oder auf die Premium-Version upgraden - Informationen dazu finden Sie in der kostenlosen VPN-Version.
- Den Server auswählen, mit dem Sie eine Verbindung herstellen möchten und die verbleibende Laufzeit Ihres Abonnements anzeigen - Informationen dazu finden Sie in der Premium-VPN-Version.

## VPN-Einstellungen

Tippen Sie auf die -Schaltfläche im VPN-Menü und wählen Sie danach **Einstellungen** für die erweiterten App-Sperre-Optionen.

Im die VPN-**Einstellungen** können Sie folgende Optionen konfigurieren:

- VPN-Schnellzugriff-Benachrichtigung – eine Benachrichtigung wird in der Statusleiste angezeigt, über die Sie VPN schnell einschalten können.
- Benachrichtigung bei Verbindung mit offenem WLAN – jedes Mal, wenn Sie eine Verbindung zu einem offenen WLAN herstellen, werden Sie in der Statusleiste darauf hingewiesen, dass Sie VPN einschalten können.
- Benachrichtigung beim Zugriff auf Online-Banking-Seiten – jedes Mal, wenn Sie eine Online-Banking-Seite aufrufen, werden Sie in der Statusleiste darauf hingewiesen, dass Sie VPN einschalten können.

## Abonnements

Mit Bitdefender VPN erhalten Sie ein kostenloses Datenvolumen von 200 MB pro Tag, um Ihre Verbindung bei Bedarf abzusichern. Sie werden automatisch mit dem besten Serverstandort verbunden.

Wenn Sie sich für ein Upgrade auf die Premium-Version entscheiden, entfällt das Datenlimit und Sie können durch die freie Wahl des Serverstandorts Inhaltsbeschränkungen überall auf der Welt umgehen.

Sie können jederzeit ein Upgrade auf Bitdefender Premium VPN vornehmen, indem Sie im Dashboard oder in der VPN-Benutzeroberfläche auf **PREMIUM VPN AKTIVIEREN** tippen.

Ein Bitdefender Premium-VPN-Abonnement läuft unabhängig von dem Bitdefender Mobile Security-Abonnement, d. h. Sie können es über den

gesamten Verfügbarkeitszeitraum hinweg nutzen, unabhängig von Status Ihres Sicherheitsabonnement Wenn Ihr Bitdefender Premium-VPN-Abonnement abläuft, Ihr Bitdefender Mobile Security-Abonnement aber weiterhin aktiv ist, kehren Sie zum kostenlosen Angebot zurück.

Bitdefender VPN ist ein plattformübergreifendes Produkt, das in Bitdefender-Produkten für Windows, macOS, Android und iOS verfügbar ist. Nach einem Premium-Upgrade können Sie Ihr Abonnement in allen Produkten nutzen, vorausgesetzt, dass Sie sich mit dem gleichen Bitdefender-Benutzerkonto anmelden.

# 26. DIEBSTAHLSCHUTZ-FUNKTIONEN

Bitdefender kann Ihnen dabei helfen, Ihr Gerät zu finden, und verhindert, dass Ihre privaten Daten in die falschen Hände gelangen.

Sie müssen nur den Diebstahlschutz über das Gerät aktivieren und können dann bei Bedarf jederzeit und mit jedem Browser auf **Bitdefender Central** zugreifen.

Durch den Versand von **SMS-Befehlen** von jedem beliebigen Mobiltelefon auf Ihr Smartphone können Sie Ihr Gerät sogar dann noch schützen, wenn Sie nicht auf das Internet zugreifen können.

Bitdefender Mobile Security bietet die folgenden Diebstahlschutzfunktionen:

**Fern-Gerätortung**
Hiermit können Sie den Standort Ihres Geräts in Google Maps anzeigen. Der Standort wird alle 5 Sekunden aktualisiert, eine Bewegung kann also nachverfolgt werden.

Die Genauigkeit der Ortung hängt davon ab, wie gut Bitdefender seinen Standort bestimmen kann:

- Wenn GPS im Gerät aktiviert ist, kann sein Standort bis auf ein paar Meter genau bestimmt werden, solange das Gerät in Reichweite der GPS-Satelliten (d. h. nicht in einem Gebäude) ist.
- Wenn sich das Gerät in einem Gebäude befindet, kann sein Standort auf mehrere zehn Meter genau bestimmt werden, solange WLAN aktiviert ist und Drahtlosnetzwerke in Reichweite des Geräts sind.
- Andernfalls wird der Standort allein über Daten aus dem Mobilfunknetzwerk bestimmt, wodurch die Genauigkeit auf einen Umkreis von ein paar hundert Metern sinkt.

**IP anzeigen**
Zeigt die letzte IP-Adresse für das ausgewählte Gerät an. Tippen Sie zum Anzeigen auf **IP ANZEIGEN**.

**Fernlöschung**
Löschen Sie alle persönlichen Daten von Ihrem Gerät.

**Fernsperrung**
Frieren Sie den Bildschirm Ihres Geräts ein, und legen Sie eine PIN fest, mit der er wieder aktiviert werden kann.

**Signal an das Gerät senden (Aufschrei)**

Sie können aus der Ferne eine Nachricht an das Gerät senden, die auf dem Bildschirm angezeigt wird, oder ein lautes Tonsignal über die Lautsprecher abspielen lassen.

Wenn Sie Ihr Gerät verlieren, können Sie den potenziellen Finder wissen lassen, wie er es Ihnen zukommen lassen kann, indem Sie auf dem Bildschirm des Geräts eine Nachricht anzeigen lassen.

Wenn Sie Ihr Gerät verlegt haben, liegt es mit einiger Wahrscheinlichkeit ganz in der Nähe (in der Wohnung oder im Büro). Sie finden es ganz leicht, indem Sie es eine lauten Ton abspielen lassen. Der Ton wird abgespielt, auch wenn das Gerät auf lautlos gestellt ist.

## Aktivierung des Diebstahlschutzes

Zur Aktivierung der Diebstahlschutzfunktionen müssen Sie nur den Konfigurationsvorgang über die Diebstahlschutz-Kachel im Dashboard abschließen.

Alternativ können Sie den Diebstahlschutz folgendermaßen aktivieren:

1. Öffnen Sie Bitdefender Mobile Security.
2. Tippen Sie auf **Menü** und wählen Sie **Diebstahlschutz** aus der Liste aus.
3. Tippen Sie auf **AKTIVIEREN**.
4. Der folgende Prozess wird eingeleitet, um Sie bei der Aktivierung dieser Funktion zu unterstützen:

   ### Beachten Sie

   Für den Diebstahlschutz werden unter Android 6 zusätzliche Berechtigungen benötigt. So können Sie ihn aktivieren:

   - Tippen Sie zunächst auf **Diebstahlschutz aktivieren** und danach auf **AKTIVIEREN**.
   - Erteilen Sie die folgenden Berechtigungen:
     a. Zulassen, dass der **Virenschutz** SMS-Nachrichten versendet und liest?
     b. Zulassen, dass der **Virenschutz** auf den Gerätestandort zugreift?
     c. Zulassen, das der **Virenschutz** auf Ihre Kontaktliste zugreift?

   a. **Administratorrechte erteilen**

Diese Rechte sind für den Betrieb des Diebstahlschutzmoduls unbedingt erforderlich und müssen eingeräumt werden, um diesen Vorgang fortzusetzen.

b. **Anwendungs-PIN festlegen**

Um sicherzustellen, dass alle Änderungen an den Diebstahlschutzeinstellungen von Ihnen autorisiert sind, muss eine PIN festgelegt werden. Diese PIN muss dann bei jeder Änderung der Diebstahlschutzeinstellungen eingegeben werden, damit die Änderungen wirksam werden. Anstelle der PIN ist bei Geräten mit Fingerabdrucksensor auch eine Bestätigung per Fingerabdruck möglich.

**Beachten Sie**

Die gleiche PIN wird von der App-Sperre verwendet, um Ihre installierten Anwendungen zu schützen.

c. **Foto aufnehmen aktivieren**

Ist Foto aufnehmen aktiviert, nimmt Bitdefender bei jedem unautorisierten Zugriff auf Ihre installierten Anwendungen ein Foto der jeweiligen Person auf. Weitere Informationen zu dieser Funktion finden Sie unter „Foto aufnehmen“ (S. 323).

d. **Vertrauenswürdige Nummer für den Diebstahlschutz vergeben**

Tippen Sie auf den Reiter **SMS-STEUERUNG**, geben Sie die Telefonnummer einer vertrauten Person ein oder wählen Sie sie aus den Kontakten aus und tippen Sie danach auf **NUMMER SPEICHERN**. Die Nummer sollte einen Ländercode enthalten und es kann sich dabei um die Nummer eines Freundes oder eines anderen von Ihnen genutzten Telefons handeln.

Wird eine neue SIM-Karte in Ihr Gerät eingelegt, schickt Bitdefender Mobile Security Ihnen automatisch eine Textnachricht mit der neuen Telefonnummer an die autorisierte Nummer.

Über diesen Weg können Sie SMS Nachrichten an Ihr Telefon versenden, obwohl die SIM Karte geändert wurde und die Nummer anders ist.

**Wichtig**

Es ist keine Pflichtangabe, aber es wird empfohlen, die vertrauenswürdige Nummer beim initialen Setup anzugeben. Der Befehl zum LÖSCHEN kann nur über die autorisierte Nummer verschickt werden.

Nach Aktivierung des Diebstahlschutzes können Sie die Funktionen zur Web- und SMS-Steuerung durch Antippen der entsprechenden Schaltflächen im Diebstahlschutzmenü einzeln aktivieren oder deaktivieren.

# Nutzung der Diebstahlschutzfunktionen über Bitdefender Central (Web-Steuerung)

### Beachten Sie

Für die Diebstahlschutz-Funktionen muss die Option **Hintergrunddaten** in den Datennutzungseinstellungen Ihres Gerätes aktiviert sein.

So können Sie über Ihr Bitdefender-Konto auf die Diebstahlschutzfunktionen zugreifen:

1. Rufen Sie Bitdefender Central auf.
2. Tippen Sie oben links auf das -Symbol und wählen Sie danach **Meine Geräte** aus.
3. Klicken Sie im Fenster **MEINE GERÄTE** auf die gewünschte Gerätekarte.
4. Wechseln Sie zum Reiter **Diebstahlschutz**.
5. Tippen Sie im unteren Feld auf das -Symbol und danach auf die Schaltfläche für die Funktion, die Sie verwenden möchten:

   **Orten** - zeigt den Standort Ihres Geräts auf Google Maps.
   **Benachrichtigung** - Sie können eine Nachricht eingeben, die auf dem Bildschirm Ihres Geräts angezeigt werden soll, und/oder das Gerät einen Ton abspielen lassen.
   **Verriegeln** - den Computer verriegeln und eine PIN zur Entriegelung festlegen.
   **Löschen** - Entfernen aller Daten auf Ihrem Gerät.

   ### Wichtig

   Nach einer Löschung funktionieren die Diebstahlschutz-Funktionen nicht mehr.

   **IP ANZEIGEN** - Zeigt die letzte IP-Adresse für das ausgewählte Gerät an.

# Nutzung der Diebstahlschutzfunktionen über SMS-Befehle (SMS-Steuerung)

Ist der SMS Befehl erstmal freigegeben, können Sie folgende Nachrichten von jedem beliebigen Telefon via SMS an Ihr Smartphone versenden.

- **LOCATE** - Senden einer Nachricht an die Rufnummer des Geräts, von dem der Befehl gesendet wurde, die den Standort des Geräts benennt. Die Nachricht beinhaltet einen Google Maps Link, welcher über den Mobile-Browser des Mobiltelefons geöffnet werden kann.
- **SCREAM** - Abspielen eines lauten Signales auf dem Gerätelautsprecher.
- **LOCK** - Den Gerätebildschirm mit der von Ihnen festgelegten PIN sperren.
- **WIPE** - alle Daten vom Gerät löschen.

  **Wichtig**
  Der Befehl zum LÖSCHEN kann nur über die autorisierte Nummer verschickt werden.

- **CALLME** - wählen der Rufnummer mit aktivierten Lautsprechern, von dem der Befehl gesendet wurde. So können Sie unbemerkt die Person belauschen, die Ihr Telefon hat.
- **HELP** - Senden einer Nachricht, die alle verfügbaren Befehle zu der Rufnummer sendet, von der diese gesendet wurde.
- **SIM Change** - An die von Ihnen festgelegte vertrauenswürdige Telefonnummer wird bei Austausch Ihrer SIM-Karte eine SMS mit der neuen Nummer gesendet. Tippen Sie auf die Option **Vertrauenswürdige Nummer**, um die Telefonnummer eines Freundes festzulegen. Sie können die Nummer von Hand eingeben oder die Person aus Ihren Kontakten auswählen.

Alle SMS Befehle müssen das folgende Format verwenden:

**bd-<PIN> <command>**

**Beachten Sie**
Die Klammern kennzeichnen Variable und sollen nicht im Befehl erscheinen.

Wenn Sie beispielsweise den Sicherheitspin auf 123456 eingestellt haben und Sie wollen eine Nachricht mit dem Standort empfangen, senden Sie die folgende Textnachricht an Ihre Rufnummer:

BD-123456 LOCATE

# 27. APP-SPERRE

Installierte Anwendungen so z.B. für E-Mail, Fotos oder Nachrichten können persönliche Daten enthalten, die Sie vor fremden Zugriff durch selektive Zugangssperren schützen können.

Mit der App-Sperre können Sie unbefugten Zugriff auf Ihre Anwendungen verhindern, indem Sie eine PIN für den Zugriff festlegen. Der PIN-Code muss 4-8 Ziffern enthalten und bei jedem Zugriff auf die zugriffsbeschränkten Anwendungen eingegeben werden.

Anstelle der PIN ist bei Geräten mit Fingerabdrucksensor auch eine Bestätigung per Fingerabdruck möglich.

## App-Sperre wird aktiviert

Um den Zugriff auf ausgewählte Anwendungen einzuschränken, können Sie die App-Sperre über die Kachel im Dashboard konfigurieren, die nach Aktivierung des Diebstahlschutzes angezeigt wird.

Alternativ können Sie die App-Sperre folgendermaßen aktivieren:

1. Öffnen Sie Bitdefender Mobile Security.
2. Tippen Sie auf **Menü** und wählen Sie **App-Sperre** aus der Liste aus.
3. Tippen Sie auf **AKTIVIEREN** und erlauben Sie danach Bitdefender den Zugriff auf die Nutzungsdaten, indem Sie die entsprechende Kästchen aktivieren.

   **Beachten Sie**
   Für die Funktion Foto aufnehmen werden unter Android 6 zusätzliche Berechtigungen benötigt.
   Erlauben Sie dem **Virenschutz** das Aufnehmen von Fotos und Videos, um sie zu aktivieren.

4. Öffnen Sie die App erneut, konfigurieren Sie den Zugriffscode und tippen Sie auf **PIN FESTLEGEN**.

   **Beachten Sie**
   Dieser Schritt steht nur zur Auswahl, wenn Sie die PIN noch nicht beim Diebstahlschutz eingerichtet haben.

5. Aktivieren Sie die Option Foto aufnehmen, um Eindringlinge zu erwischen, die versuchen, auf Ihre privaten Daten zuzugreifen.
6. Wählen Sie die Apps aus, die Sie schützen möchten.

Wird fünf Mal in Folge die falsche PIN eingegeben oder der falsche Fingerabdruck verwendet, tritt eine 30-sekündige Sperre ein. Auf diese Weise werden Versuche, auf geschützte Apps zuzugreifen unterbunden.

**Beachten Sie**
Die gleiche PIN wird vom Diebstahlschutz verwendet, um den Standort Ihres Geräts zu ermittelt.

App-Sperre

## Sperrmodus

Hier können Sie entscheiden, wann die App-Sperre die auf Ihrem Gerät installierten Anwendungen schützen soll.

Ihnen stehen die folgenden Optionen zur Auswahl:

- **Jedes Mal sperren** - PIN oder Fingerabdruck werden für jeden Zugriff auf die gesperrten Apps abgefragt.
- **Bis zur Bildschirmabschaltung entsperrt lassen** - Sie können bis zur nächsten Bildschirmabschaltung auf die Apps zugreifen.
- **Kurzzeitiges Verlassen erlauben** - Sie können entsperrte Apps verlassen und innerhalb von 30 Sekunden wieder aufrufen.
- **Intelligentes Entsperren** - Bei Aktivierung dieser Option und Verbindung mit einem als vertrauenswürdig eingestuften Netzwerk sind die anderen Einstellungen nicht verfügbar. Beim Zugriff auf gesperrte Apps werden PIN oder Fingerabdruck also nicht abgefragt.

## App-Sperre-Einstellungen

Tippen Sie auf die -Schaltfläche im App-Sperre-Menü und wählen Sie danach **Einstellungen** für die erweiterten App-Sperre-Optionen.

In den App-Sperre-**Einstellungen** ist Folgendes möglich:

- Foto nach 3 fehlgeschlagenen Entsperrversuchen aufnehmen aktivieren.
- Sperrbenachrichtigungen für neu installierte Apps.
- Ändern Sie Ihre PIN.

## Foto aufnehmen

Mit der Foto-aufnehmen-Funktion von Bitdefender erwischen Sie Ihre Freunde oder Verwandten auf frischer Tat. So können Sie ihnen klar machen, dass Ihre persönlichen Dateien und installierten Anwendungen nicht für Ihre Augen bestimmt sind.

Es funktioniert ganz einfach: Wird dreimal hintereinander die falsche PIN oder der falsche Fingerabdruck eingegeben, wird mit der Frontkamera ein Foto aufgenommen. Das Foto wird dann mit Zeitstempel und einem Hinweis

auf den Aufnahmegrund gespeichert und kann in Bitdefender Mobile Security über die App-Sperre-Funktion angezeigt werden.

**Beachten Sie**
Diese Funktion steht nur auf Telefonen mit Frontkamera zur Verfügung.

So konfigurieren Sie die Foto-aufnehmen-Funktion:

1. Öffnen Sie Bitdefender Mobile Security.
2. Tippen Sie auf **Menü** und wählen Sie **App-Sperre** aus der Liste aus.
3. Tippen Sie auf die -Schaltfläche im App-Sperre-Menü und wählen Sie **Einstellungen** aus.
4. Aktivieren Sie die Option **Foto nach 3 fehlgeschlagenen Entsperrversuchen aufnehmen**

Die Fotos, die nach Eingabe einer falschen PIN aufgenommen werden, werden im App-Sperre-Menü angezeigt und können dort als Vollbild eingesehen werden.

Alternativ können Sie diese auch über Ihr Bitdefender-Konto anzeigen:

1. Gehen Sie zu: https://central.bitdefender.com.
2. Melden Sie sich bei Ihrem Konto an.
3. Tippen Sie oben links auf das -Symbol und wählen Sie danach **Meine Geräte** aus.
4. Wählen Sie Ihr Gerät über das Fenster **MEINE GERÄTE** und den Reiter **Diebstahlschutz** aus.

   Die Fotos werden angezeigt.

Es werden nur die 3 aktuellsten Fotos gespeichert.

## Intelligentes Entsperren

Damit die App-Sperre Sie nicht bei jedem Aufrufen einer geschützten App nach Ihrer PIN oder Ihrem Fingerabdruck fragt, können Sie das intelligente Entsperren aktivieren.

Mit der Funktion für das intelligente Entsperren können Sie vertrauenswürdige WLAN-Netzwerke festlegen. Bei Verbindung mit einem dieser Netzwerke

werden die Blockierungseinstellungen der App-Sperre für die geschützten Apps deaktiviert.

So können Sie das Intelligente Entsperren aktivieren:

1. Öffnen Sie Bitdefender Mobile Security.
2. Tippen Sie auf **Menü** und wählen Sie **App-Sperre** aus der Liste aus.
3. Rufen Sie den Reiter **SPERRMODUS** auf und aktivieren Sie den entsprechenden Schalter.

   Das gerade verwendete WLAN-Netzwerk wird angezeigt.

   Tippen Sie auf das -Symbol, um die aktuell genutzte WLAN-Verbindung als vertrauenswürdig einzustufen.

**Beachten Sie**
Um diese Einstellung vorzunehmen, muss das intelligente Entsperren aktiviert sein.

Falls Sie es sich anders überlegen, können Sie die Funktion jederzeit deaktivieren. Alle bisher als vertrauenswürdig eingestuften WLAN-Netzwerke gelten dann wieder als nicht vertrauenswürdig.

# 28. BERICHTE

Die Berichtsfunktion protokolliert alle Ereignisse im Zusammenhang mit den Scans auf Ihrem Gerät.

Für jedes sicherheitsrelevante Ereignis auf Ihrem Gerät wird den Berichten eine neue Nachricht hinzugefügt.

So können Sie auf den Bereich Berichte zugreifen:

1. Öffnen Sie Bitdefender Mobile Security.
2. Tippen Sie auf **Menü** und wählen Sie **Berichte** aus der Liste aus.

Im Fenster Berichte finden Sie die folgenden Reiter:

- **WÖCHENTLICHE BERICHTE** - Hier können Sie den Sicherheitsstatus und die durchgeführten Aktionen für die aktuelle und vorausgegangene Woche einsehen. Der Bericht für die aktuelle Woche wird jeweils Sonntags erstellt. Sie werden informiert, sobald der Bericht verfügbar ist.

  In diesem Bereich wird jede Woche ein neuer Hinweis angezeigt. Schauen Sie also regelmäßig vorbei, um optimalen Nutzen aus der App zu ziehen.

- **AKTIVITÄTSPROTOKOLL** - Hier können Sie ausführliche Informationen zu den Aktivitäten Ihrer Bitdefender Mobile Security-App seit Installation auf Ihrem Android-Gerät einsehen.

  Tippen Sie auf die -Schaltfläche oben rechts auf Ihrem Bildschirm und wählen Sie danach **Aktivitätsprotokoll leeren** aus, um das vorliegende Aktivitätsprotokoll zu löschen.

# 29. WEARON

Mit Bitdefender-WearON können Sie Ihr Smartphone schnell und einfach wiederfinden, egal ob Sie es bei der Arbeit im Besprechungsraum oder unter eine Kissen auf dem Sofa vergessen haben. Das Gerät lässt sich auch dann aufspüren, wenn es auf lautlos gestellt ist.

Lassen Sie diese Funktion aktiviert, damit Sie Ihr Smartphone jederzeit zur Hand haben.

**Beachten Sie**
Diese Funktion benötigt Android 4.3 und Android Wear.

## Aktivierung von WearON

Zur Verwendung von WearON müssen Sie Ihre Smartwatch mit der Bitdefender Mobile Security-Anwendungen verbinden und die Funktion über den folgenden Sprachbefehl aktivieren:

**Start:<Where is my phone>**

**Bitdefender-WearON** kennt zwei Befehle:

1. **Mobile-Warnung**

   Mit der Phone-Alert-Funktion können Sie Ihr Smartphone schnell wiederfinden, wenn Sie sich zu weit davon entfernt haben.

   Wenn Sie Ihre Smartwatch tragen, erkennt sie automatisch die Anwendung auf Ihrem Telefon und vibriert, sobald Sie sich mehr als zehn Meter von Ihrem Telefon entfernen.

   Öffnen Sie zur Aktivierung dieser Funktion Bitdefender Mobile Security, tippen Sie im Menü auf **Allgemeine Einstellungen** und wählen Sie im Bereich WearON den entsprechenden Schalter aus.

2. **Scream**

   Es war noch nie so einfach, Ihr Telefon aufzuspüren. Sie haben vergessen, wo Ihr Telefon liegt? Tippen Sie einfach auf den Scream-Befehl auf Ihrer Uhr, um den Scream-Alarm auszulösen.

# 30. EINSTELLUNGEN

Im Bereich Einstellungen können Sie die folgenden Optionen anpassen:

- **Sicherheits-PIN** - Hier können Sie den PIN-Code ändern, den Sie für die App-Sperre oder die Diebstahlschutzbefehle festgelegt haben.
- **Virenscanner** - Hier können Sie festlegen, ob der Speicher geprüft werden soll.
- **In-the-Cloud-Erkennung** - Hier können Sie festlegen, ob uns Berichte übermittelt werden, die uns bei der Verbesserung der Cloud-Erkennung unterstützen.
- **Kontoschutz** - Hier können Sie festlegen, ob Sie auch informiert werden möchten, wenn Ihre Benutzerkonten von Datenlecks nicht betroffen sind.
- **App-Sperre** - Hier können Sie festlegen, ob für neu installierte Apps Sperrbenachrichtigungen angezeigt werden sollen.
- **Foto aufnehmen** - Hier können Sie festlegen, ob nach drei fehlgeschlagenen App-Aufrufen ein Foto aufgenommen werden soll.
- **Diebstahlschutz** - Hier können Sie die vertrauenswürdige Telefonnummer ändern, die Sie für den Fall angegeben haben, dass Ihr Gerät in fremde Hände gerät.
- **Berichte** - Hier können Sie festlegen, ob Sie Benachrichtigungen zu Berichten erhalten möchten.
- **Anonyme Nutzungsstatistiken senden** - Hier können Sie festlegen, ob uns Berichte mit Informationen zu Ihrer Produktnutzung übermittelt werden. Diese Information ist wichtig für die Verbesserung des Produktes.

# 31. INFO ÜBER

Informationen zur installierten Bitdefender Mobile Security-Version finden Sie im Bereich **Info über**. Hier können Sie uns auch mit Support-Anfragen kontaktieren, die Abonnementvereinbarung sowie die Datenschutzrichtlinie aufrufen und lesen sowie die Open-Source-Lizenzen anzeigen.

# 32. BITDEFENDER CENTRAL

Bitdefender Central stellt Ihnen eine Web-Plattform zur Verfügung, über die Sie auf die Online-Funktionen und -Dienste des Produkts zugreifen und wichtige Aufgaben auf allen Geräten ausführen können, auf denen Bitdefender installiert ist. Über https://central.bitdefender.com können Sie sich mit jedem internetfähigen Computer oder Mobilgerät bei Ihrem Bitdefender-Konto anmelden. Nachdem Sie es aufgerufen haben, stehen Ihnen die folgenden Optionen zur Verfügung:

- Laden Sie Bitdefender herunter und installieren Sie es auf Windows-, macOS-, iOS- und Android-Betriebssystemen. Die folgenden Produkte stehen zum Download bereit:
  - Bitdefender Mobile Security
  - Bitdefender Mobile Security for iOS
  - Bitdefender Antivirus for Mac
  - Die Bitdefender-Windows-Produktlinie
- Verwaltung und Verlängerung Ihrer Bitdefender-Abonnements.
- Neue Geräte zu Ihrem Netzwerk hinzufügen und diese Geräte aus der Ferne verwalten.

## Aufrufen Ihres Bitdefender-Benutzerkontos.

So können Sie Ihr Bitdefender-Benutzerkonto bequem aufrufen:

1. Öffnen Sie einen Web-Browser auf jedem beliebigen internetfähigen Gerät.
2. Gehen Sie zu: https://central.bitdefender.com.
3. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Konto an.

## Meine Geräte

Über Ihr Bitdefender-Benutzerkonto können Sie im Bereich **Meine Geräte** die Bitdefender-Produkte auf Ihren Geräten aus der Ferne installieren und verwalten, sofern die Geräte eingeschaltet und mit dem Internet verbunden sind. Auf den Gerätekacheln sind der Gerätename, der Sicherheitsstatus angegeben sowie die Information, ob Sicherheitsprobleme auf Ihren Geräten bestehen.

Sie können Gerätenamen vergeben, um die Geräte später leichter identifizieren zu können:

1. Rufen Sie Bitdefender Central auf.
2. Tippen Sie oben links auf das ☰-Symbol und wählen Sie danach **Meine Geräte** aus.
3. Tippen Sie auf die gewünschte Gerätekachel und dann auf das Symbol ⋮ in der rechten oberen Ecke.
4. Tippen Sie auf **Einstellungen**.
5. Geben Sie einen neuen Namen in das Feld **Gerätename** ein und tippen Sie dann auf **SPEICHERN**.

Sie können für jedes Ihrer Geräte zur einfacheren Verwaltung einen Besitzer anlegen und zuordnen:

1. Rufen Sie Bitdefender Central auf.
2. Tippen Sie oben links auf das ☰-Symbol und wählen Sie danach **Meine Geräte** aus.
3. Tippen Sie auf die gewünschte Gerätekachel und dann auf das Symbol ⋮ in der rechten oberen Ecke.
4. Wählen Sie **Profil**.
5. Tippen Sie auf **Besitzer hinzufügen** und füllen Sie dann die entsprechenden Felder aus. Passen Sie das Profil nach Bedarf an, indem Sie ein Foto hinzufügen und einen Geburtstag eingeben.
6. Tippen Sie auf **HINZUFÜGEN**, um das Profil zu speichern.
7. Wählen Sie aus der **Gerätebesitzer**-Liste den gewünschten Besitzer aus und tippen Sie auf **ZUORDNEN**.

Wählen Sie die entsprechende Gerätekarte aus, um das Gerät per Fernzugriff zu steuern oder Informationen zu Ihrem Bitdefender-Produkt auf einem bestimmten Geräte anzuzeigen.

Wählen Sie eine Gerätekarte aus, um die folgenden Reiter anzuzeigen:

- **Dashboard** . In diesem Fenster können Sie Details zum ausgewählten Gerät anzeigen, den Schutzstatus sowie den Status des Bitdefender VPN und die Zahl der blockierten Bedrohungen der letzten sieben Tage einsehen. Der Sicherheitsstatus ist grün, wenn es keine Sicherheitsprobleme gibt,

gelb, wenn es etwas gibt, was Ihre Aufmerksamkeit erfordert, und rot, wenn Ihr Gerät gefährdet ist. Gibt es Probleme, die sich auf Ihr Gerät auswirken, tippen Sie im oberen Statusbereich auf den Drop-down-File, um weitere Details anzuzeigen. Von hier aus können die Probleme, die Ihre Gerätesicherheit beeinträchtigen, manuell behoben werden.

- **Schutz**. Von diesem Fenster aus können Sie einen Scan oauf Ihrem Gerät durchführen. Klicken Sie dazu auf die Schaltfläche **SCANNEN**. Sie können auch nachvollziehen, wann der letzte Scan auf dem Gerät durchgeführt wurde, und einen Bericht für den aktuellsten Scan abrufen, in dem die wichtigsten Informationen zusammengefasst werden.
- **Diebstahlschutz**. Falls Sie Ihr Gerät verlegt haben, können Sie es mit der Diebstahlschutzfunktion wiederfinden und aus der Ferne steuern. Klicken Sie auf **ORTEN**, um die Position des Gerätes zu bestimmen. Die letzte bekannte Position wird mit Datum und Tageszeit angezeigt. Weitere Informationen zu dieser Funktion finden Sie unter *„Diebstahlschutz-Funktionen“* (S. 315).

# Meine Abonnements

Über die Bitdefender Central-Plattform können Sie bequem die Abonnements für alle Ihre Geräte verwalten.

# Verfügbare Abonnements anzeigen

So können Sie Ihre verfügbaren Abonnements anzeigen:

1. Rufen Sie Bitdefender Central auf.
2. Tippen Sie oben links auf das ☰-Symbol und wählen Sie danach **Meine Abonnements** aus.

Hier werden alle Informationen zur Verfügbarkeit Ihrer Abonnements und die Anzahl der Geräte angezeigt, auf denen diese verwendet werden.

Klicken Sie auf eine Abonnementkarte, um Ihrem Abonnement ein neues Gerät hinzuzufügen oder es zu verlängern.

# Ein neues Gerät hinzufügen

Falls Ihr Abonnement mehr als ein Gerät umfasst, können Sie ein neues Gerät hinzufügen und darauf Ihr Bitdefender Mobile Security installieren. Weitere

Informationen dazu finden Sie im Abschnitt „Installation von Bitdefender Mobile Security“ (S. 299).

## Abonnement verlängern

Wenn in Ihrem Abonnement noch weniger als 30 Tage verbleiben und Sie sich gegen eine automatische Verlängerung entschieden haben, können Sie Ihr Abonnement wie folgt auch manuell verlängern:

1. Rufen Sie Bitdefender Central auf.
2. Tippen Sie oben links auf das ☰-Symbol und wählen Sie danach **Meine Abonnements** aus.
3. Wählen Sie die gewünschte Abonnementkarte aus.
4. Klicken Sie zum Fortfahren auf **VERLÄNGERN**.

In Ihrem Web-Browser wird eine neue Seite geöffnet, über die Sie Ihr Bitdefender-Abonnement verlängern können.

# 33. HÄUFIG GESTELLTE FRAGEN

**Wieso benötigt Bitdefender Mobile Security eine Internet-Verbindung?**

Die Anwendung muss mit den Bitdefender-Servern kommunizieren, um den Sicherheitsstatus der Anwendungen, die gescannt werden, und der Webseiten, die Sie besuchen, zu bestimmen. Darüber hinaus erhält es so die Befehle, die bei Verwendung der Diebstahlschutzfunktionen über Ihr Bitdefender-Konto verschickt werden.

**Wofür werden die einzelnen Berechtigungen von Bitdefender Mobile Security benötigt?**

- Internet-Zugang -> für die Cloud-Kommunikation.
- Gerätstatus und Identität ermitteln -> hiermit wird ermittelt, ob Ihr Gerät mit dem Internet verbunden ist, und bestimmte Geräteinformationen ausgelesen, die nötig sind, um eine einzigartige ID für die Kommunikation mit der Bitdefender-Cloud zu erstellen.
- Browser-Lesezeichen anlegen und benutzen -> Der Surfschutz löscht schädliche Websites aus dem Browser-Verlauf.
- Protokolle lesen -> Bitdefender Mobile Security kann anhand der Android-Protokolle Bedrohungsaktivitäten erkennen.
- SMS lesen/schreiben, Kontakte, Kontoinformationen und externe Speicher -> wird für die Fernlösch-Funktion benötigt.
- Ortung -> für die Fern-Geräteortung.
- Kamera -> wird für die Funktion Foto aufnehmen benötigt.
- Speicher -> wird benötigt, um dem Virenscanner die Prüfung der SD-Karte zu erlauben.

**Wo kann ich Einzelheiten zu den Aktivitäten der App einsehen?**

Bitdefender Mobile Security führt ein Protokoll über alle wichtigen Aktionen, Statusänderungen und andere kritische Nachrichten über die eigenen Aktivitäten. Rufen Sie diese Informationen auf, indem Sie Bitdefender Mobile Security öffnen und auf die **Menü**-Schaltfläche tippen. Wählen Sie **Berichte** aus der Liste aus.

**Ich habe den PIN-Code vergessen, mit dem ich meine Anwendung geschützt habe. Was muss ich tun?**

1. Rufen Sie Bitdefender Central auf.
2. Tippen Sie oben links auf das -Symbol und wählen Sie danach **Meine Geräte** aus.
3. Tippen Sie auf die gewünschte Gerätekachel und dann auf das Symbol in der rechten oberen Ecke.
4. Tippen Sie auf **Einstellungen**.
5. Sie können den PIN-Code im Feld **Anwendungs-PIN** abrufen.

**Wie wirkt sich Bitdefender Mobile Security auf die Systemleistung und Akkulaufzeit meines Geräts aus?**

Die Auswirkungen sind minimal. Die Anwendung läuft nur, wenn es absolut notwendig ist, d.h. wenn Sie sie installieren, wenn Sie die Anwendung aufrufen oder eine Sicherheitsprüfung durchführen. Bitdefender Mobile Security läuft nicht im Hintergrund, wenn Sie Ihre Freunde anrufen, Nachrichten schreiben oder Spiele spielen.

**Wie kann ich die App-Sperre deaktivieren?**

Es gibt keine eigene Option zur Deaktivierung der App-Sperre, Sie müssen dazu lediglich die Kästchen neben den ausgewählten Apps deaktivieren. Dazu wird die festgelegte PIN oder der Fingerabdruck abgefragt.

**Wie kann ich ein weiteres WLAN-Netzwerk als vertrauenswürdig einstufen?**

So können Sie ein weiteres WLAN-Netzwerk als vertrauenswürdig festlegen:

1. Öffnen Sie Bitdefender Mobile Security.
2. Tippen Sie auf **Menü** und wählen Sie **App-Sperre** aus der Liste aus.
3. Rufen Sie den Reiter **SPERRMODUS** auf und tippen Sie danach auf das -Symbol.
4. Bestätigen Sie Ihre Auswahl mit Ihrer PIN oder Ihrem Fingerabdruck.
5. Tippen Sie auf das -Symbol neben dem Netzwerk, das Sie als vertrauenswürdig einstufen möchten.

**Wie deaktiviere ich die Anzeige von Fotos, die mit meinem Gerät aufgenommen wurden?**

So können Sie die Anzeige von Fotos deaktivieren, die mit Ihren Geräten aufgenommen wurden:

1. Rufen Sie Bitdefender Central auf.
2. Tippen Sie oben rechts auf dem Bildschirm auf das Symbol .
3. Tippen Sie im Menü auf **Mein Konto**.
4. Wechseln Sie zum Reiter **Einstellungen**.
5. Deaktivieren Sie die Option **Mit Ihren Geräten aufgenommene Fotos anzeigen/nicht anzeigen**.

**Wie kann ich sicher im Netz einkaufen und bezahlen?**

Online-Einkäufe sind mit großen Risiken verbunden, wenn einige Details übersehen werden. Um zu verhindern, dass auch Sie zum Betrugsopfer werden, sollten Sie folgende Empfehlungen beachten:

- Halten Sie Ihre Sicherheitslösung immer auf dem neuesten Stand.
- Stellen Sie bei Online-Zahlungen sicher, dass Käuferschutz gewährleistet wird.
- Nutzen Sie in öffentlichen und ungesicherten WLAN-Netzwerken eine VPN-Verbindung zur Verbindung mit dem Internet.
- Prüfen Sie die Passwörter Ihrer Online-Benutzerkonten. Stellen Sie sicher, dass sie neben Groß- und Kleinbuchstaben auch Zahlen und Sonderzeichen (@, !, %, # usw.) enthalten.
- Übermitteln Sie Informationen ausschließlich über sichere Verbindungen. Achten Sie darauf, dass die Adresse der Website mit HTTPS:// und nicht mit HTTP:// beginnt.

**Wann sollte ich Bitdefender VPN nutzen?**

Bei Aufrufen, Herunterladen oder Hochladen von Inhalten im Internet sollten Sie stets Vorsicht walten lassen. Um sicherzustellen, dass Sie beim Surfen im Netz jederzeit geschützt sind, empfehlen wie den Einsatz von Bitdefender VPN, wenn Sie:

- Verbindungen zu öffentlichen WLAN-Netzwerken herstellen möchten
- auf Inhalte zugreifen möchten, die regionalen Zugangsbeschränkungen unterliegen, egal ob zuhause oder im Ausland
- Ihre persönlichen Daten vor Zugriff schützen möchten (Benutzernamen, Passwörter, Kreditkartendaten etc.)
- Ihre IP-Adresse verbergen möchten

**Wirkt sich Bitdefender VPN auf die Akkulaufzeit meines Gerätes aus?**

Bitdefender VPN wurde eigens entwickelt, um Ihre persönlichen Daten zu schützen, Ihre IP-Adresse bei Verbindungen mit ungesicherten WLAN-Netzwerken zu verbergen und Ihnen den Zugriff auf Inhalte mit länderspezifischen Zugangsbeschränkungen zu ermöglichen. Um Ihren Akku zu entlasten, empfehlen wir, das VPN nur bei Bedarf zu nutzen und die Verbindung danach wieder zu trennen.

**Wird meine Internetverbindung langsamer, wenn ich eine Verbindung mit Bitdefender VPN herstelle?**

Bitdefender VPN ist auf einen ressourcenschonenden Betrieb beim Surfen im Netz ausgelegt. Ihre Internetverbindung bzw. die Entfernung zu Server, mit dem Sie eine Verbindung hergestellt haben, können sich jedoch negativ auf die Verbindungsgeschwindigkeit auswirken. Wenn es nicht unbedingt notwendig ist, dass Sie sich von Ihrem Standort aus mit einem weit entfernten Server verbinden (z. B. von Deutschland aus nach China), sollten Sie in solchen Fällen Bitdefender VPN erlauben, automatisch eine Verbindung mit dem nächstgelegenen Server herzustellen bzw. einen Server zu finden, der näher an Ihrem Standort liegt.

**Kann ich das Bitdefender-Konto ändern, das mit meinem Gerät verknüpft ist?**

Ja, Sie können jederzeit Ihrem Gerät ein anderes Bitdefender-Konto zuordnen. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie Bitdefender Mobile Security.
2. Tippen Sie auf **Menü** und wählen Sie **Mein Konto** aus der Liste aus.
3. Tippen Sie auf **ABMELDEN** und bestätigen Sie Ihre Auswahl.
4. Tippen Sie auf **CENTRAL-KONTO VERWENDEN** und geben Sie danach Ihre neue Bitdefender-E-Mail-Adresse und Ihr Passwort ein.

**Was ist Geräteadministratoren?**

Geräteadministratoren ist eine Android-Funktion, über die Bitdefender Mobile Security die Berechtigungen erhält, die es zur Ausführung bestimmter Aktionen aus der Ferne benötigt. Ohne diese Rechte könnte die Fernsperrung nicht funktionieren, und die Fernlöschung könnte Ihre Daten nicht löschen. Sollten Sie die App entfernen wollen, müssen Sie vor der Deinstallation diese Rechte wieder entziehen über **Einstellungen > Sicherheit > Geräteadministratoren auswählen**.

**Wofür wird die autorisierte Nummer benötigt?**

Falls Ihr Telefon jemandem in die Hände fällt, der keinerlei Absichten hat, es dem rechtmäßigen Besitzer zurückzugeben, ist es sehr wahrscheinlich, dass Ihre SIM-Karte umgehend ausgetauscht wird. Sobald Bitdefender Mobile Security eine neue SIM-Karte in Ihrem Telefon erkennt, schickt es automatisch eine Textnachricht mit der neuen Nummer an die von Ihnen festgelegte Nummer. Über diesen Weg können Sie SMS Nachrichten an Ihr Telefon versenden, obwohl die SIM Karte geändert wurde und die Nummer anders ist. Sie können dafür die Nummer einer vertrauten Person oder auch die Nummer eines weiteren von Ihnen genutzten Telefons verwenden.

**Kann die autorisierte Nummer später auch wieder geändert werden?**

So legen Sie eine neue vertrauenswürdige Nummer fest:

1. Öffnen Sie Bitdefender Mobile Security.
2. Tippen Sie auf **Menü** und wählen Sie **Einstellungen** aus der Liste aus.
3. Tippen Sie im Bereich **Diebstahlschutz** auf **Vertrauenswürdige Nummer**.

   Bevor Sie die autorisierte Nummer ändern können, müssen Sie die PIN eingeben.

**Was kostet mich der Versand von SMS-Befehlen?**

SMS-Befehle werden als herkömmliche Textnachrichten versandt und werden auch als solche von Ihrem Anbieter abgerechnet. Durch Bitdefender entstehen Ihnen keine zusätzlichen Kosten.

**So beheben Sie den "Keine Google-Token"-Fehler, der bei der Bitdefender Mobile Security-Anmeldung auftritt.**

Dieser Fehler tritt auf, wenn das Gerät mit keinem Google-Konto verknüpft ist oder wenn es zwar mit einem Konto verknüpft ist, es aber wegen eines vorübergehenden Problems keine Verbindung zu Google herstellen kann. Die folgenden Schritte können das Problem beheben:

- Öffnen Sie die Android-Einstellungen und gehen Sie danach auf > Anwendungen > Anwendungsmanager > Bitdefender Mobile Security und tippen Sie auf **Daten löschen**. Melden Sie sich dann erneut an.
- Ihr Gerät muss mit einem Google-Konto verknüpft sein.

  Ob es das ist, können Sie wie folgt überprüfen: Gehen Sie zu Einstellungen > Konten & Synchronisierung, und sehen Sie nach, ob unter **Konten verwalten** ein Google-Konto aufgeführt ist. Fügen Sie Ihr Konto hinzu; falls

kein Konto aufgeführt ist, starten Sie Ihr Gerät neu und versuchen Sie dann, sich bei Bitdefender Mobile Security anzumelden.

- Starten Sie Ihr Gerät neu, und versuchen Sie es dann erneut.

**In welchen Sprachen ist Bitdefender Mobile Security verfügbar?**

Bitdefender Mobile Security ist derzeit in den folgenden Sprachen verfügbar:

- Brasilianisch
- Tschechisch
- Niederländisch
- Englisch
- Französisch
- Deutsch
- Griechisch
- Ungarisch
- Italienisch
- Japanisch
- Koreanisch
- Polnisch
- Portugiesisch
- Rumänisch
- Russisch
- Spanish
- Thai
- Türkisch
- Vietnamesisch

Weitere Sprachen werden in zukünftigen Versionen hinzugefügt. Sie können die Sprache von Bitdefender Mobile Security ändern, indem Sie unter **Sprache & Tastatur** die gewünschte Sprache für Ihr Gerät einstellen.

# KONTAKTIEREN SIE UNS

# 34. HILFE ANFORDERN

Bitdefender bietet seinen Kunden konkurrenzlos schnellen und kompetenten Support. Sollten sich Probleme ergeben oder Sie eine Frage zu Ihrem Bitdefender-Produkt haben, so stehen Ihnen verschiedene Online-Quellen zur Verfügung, wo Sie Lösungen und Antworten finden. Sie können sich auch jederzeit an den Bitdefender-Kundendienst wenden. Unsere Kundenbetreuer beantworten Ihre Fragen zügig und bieten Ihnen die benötigte Unterstützung.

Im Abschnitt *„Verbreitete Probleme beheben“* (S. 200) finden Sie alle wichtigen Informationen zu den häufigsten Problemen, die bei der Verwendung dieses Produkts auftreten können.

Wenn Sie in den vorhandenen Quellen keine Antwort auf Ihre Frage finden, können Sie uns direkt kontaktieren:

- „Kontaktieren Sie uns direkt aus Ihrem Bitdefender Total Security 2018-Produkt heraus“ (S. 341)
- „Kontaktieren Sie uns über unser Online-Support-Center“ (S. 342)

## Kontaktieren Sie uns direkt aus Ihrem Bitdefender Total Security 2018-Produkt heraus

Wenn Sie über eine aktive Internet-Verbindung verfügen, können Sie Bitdefender direkt aus der Benutzeroberfläche heraus kontaktieren, um Hilfe zu erhalten.

Folgen Sie diesen Schritten:

1. Klicken Sie im linken Seitenbereich der Bitdefender-Benutzeroberfläche auf das -Symbol.
2. Sie haben die folgenden Möglichkeiten:
   - **BENUTZERHANDBUCH**

     Hier können Sie unsere Datenbank nach den gewünschten Informationen durchsuchen.
   - **SUPPORT-CENTER**

     Greifen Sie auf unsere Online-Artikel und Videoanleitungen zu.
   - **Support kontaktieren**

Sie können über die Schaltfläche **KUNDENDIENST KONTAKTIEREN** das Bitdefender-Support-Tool aufrufen und den Kundendienst kontaktieren.

a. Geben Sie in das Formular die nötigen Daten ein:

   i. Wählen Sie die Art des aufgetretenen Problems.

   ii. Beschreiben Sie im Textfeld das Problem, das aufgetreten ist.

   iii. Klicken Sie auf **DAS PROBLEM REPRODUZIEREN**, falls Probleme mit dem Produkt aufgetreten sind. Fahren Sie mit den erforderlichen Schritten fort.

   Warten Sie einen Moment, während Bitdefender die produktrelevanten Informationen einholt. Diese Informationen helfen unseren Mitarbeitern, eine Lösung für Ihr Problem zu finden.

   iv. Klicken Sie auf **TICKET BESTÄTIGEN**.

b. Vervollständigen Sie das Übermittlungsformular mit den benötigten Informationen:

   i. Geben Sie Ihren vollen Namen ein.

   ii. Geben Sie Ihre E-Mail-Adresse ein.

   iii. Markieren Sie das Einverständniskästchen.

   iv. Kicken Sie auf **TICKET ABSCHICKEN**.

   Warten Sie einen Moment, während Ihr Ticket erstellt wird und die gesammelten Informationen an den Bitdefender-Kundendienst übermittelt werden.

c. Klicken Sie auf **SCHLIEßEN**, um den Assistenten zu beenden. Einer unserer Mitarbeiter wird sich so schnell wie möglich mit Ihnen in Verbindung setzen.

## Kontaktieren Sie uns über unser Online-Support-Center

Wenn Sie über das Bitdefender-Produkt nicht auf die notwendigen Informationen zugreifen können, wenden Sie sich bitte an unser Online-Support-Center.

1. Gehen Sie zu http://www.bitdefender.de/support/consumer.html.

Im Bitdefender-Support-Center finden Sie eine Vielzahl von Beiträgen, die Lösungen zu Problemen im Zusammenhang mit Bitdefender bereithalten.

2. Nutzen Sie die Suchleiste oben im Fenster, um Artikel zu finden, die eine Lösung für Ihr Problem enthalten könnten. Geben Sie dazu einen Begriff in die Suchleiste ein und klicken Sie auf **Suchen**.
3. Lesen Sie die relevanten Artikel oder Dokumente und probieren Sie die vorgeschlagenen Lösungen aus.
4. Wenn die dort vorgeschlagene Lösung das Problem nicht behebt, gehen Sie zu

   http://www.bitdefender.de/support/contact-us.htmlund kontaktieren Sie unseren Kundendienst.

# 35. ONLINE-RESSOURCEN

Für die Lösung Ihres Problems und Fragen im Zusammenhang mit Bitdefender stehen Ihnen verschiedene Online-Ressourcen zur Verfügung.

- Bitdefender-Support-Center:

  http://www.bitdefender.de/support/consumer.html

- Bitdefender Support-Forum:

  http://forum.bitdefender.com

- Das Computer-Sicherheitsportal HOTforSecurity:

  http://www.hotforsecurity.com

Zudem können Sie auch Ihre favorisierte Suchmaschine nutzen, um mehr zu erfahren über Computersicherheit, die Bitdefender-Produkte und das Unternehmen.

## 35.1. Bitdefender-Support-Center

Das Bitdefender-Support-Center ist eine Online-Sammlung von Informationen zu Ihren Bitdefender-Produkten. Hier sind in einem leicht zugänglichen Format Berichte zu den Ergebnissen des fortlaufenden technischen Supports sowie der Bugfix-Aktivitäten der Bitdefender-Support- und Entwicklungsteams gespeichert. Hinzu kommen Artikel zur Bedrohungsvorbeugung, detaillierte Erklärungen zur Verwaltung von Bitdefender-Lösungen und vieles mehr.

Das Bitdefender-Support-Center ist öffentlich zugänglich und frei durchsuchbar. Die darin enthaltenen Informationen sind äußerst umfangreich und stellen eine weitere Methode dar, mit der Bitdefender-Kunden mit dem notwendigen technischen Wissen versorgt werden. Alle berechtigen Informationsanfragen oder Fehlermeldungen von Bitdefender-Kunden finden sich über kurz oder lang im Bitdefender-Support-Center wieder und dienen als Bugfix-Anleitungen, Umgehungslösungen oder Informationsartikel, die die Hilfedateien des Produkts ergänzen sollen.

Das Bitdefender-Support-Center steht Ihnen jederzeit unter der folgenden Adresse zur Verfügung:

http://www.bitdefender.de/support/consumer.html.

## 35.2. Bitdefender Support-Forum

Das Bitdefender Support-Forum bietet Bitdefender-Anwendern eine Möglichkeit, Hilfe zu erhalten oder anderen Hilfestellung zu geben.

Falls Ihr Bitdefender-Produkt nicht richtig funktioniert, bestimmte Bedrohungen nicht von Ihrem Computer entfernen kann oder wenn Sie Fragen über die Funktionsweise haben, stellen Sie Ihr Problem oder Frage in das Forum ein.

Support-Techniker von Bitdefender überwachen neue Einträge in das Forum, um Ihnen helfen zu können. Außerdem können Sie eine Antwort auf Ihre Frage oder einen Lösungsvorschlag von einem bereits erfahrenen Bitdefender-Anwender erhalten.

Bevor Sie einen Eintrag ins Forum stellen, suchen Sie im Forum nach einem ähnlichen oder verwandten Themenbereich.

Das Bitdefender Support-Forum finden Sie unter http://forum.bitdefender.com. Es steht in 5 verschiedenen Sprachen zur Verfügung: Englisch, Deutsch, Französisch, Spanisch und Rumänisch. Für den Zugriff auf den Bereich Konsumgüter klicken Sie bitte auf **Schutz für Privatanwender**.

## 35.3. Das Portal HOTforSecurity

HOTforSecurity bietet umfangreiche Informationen rund um das Thema Computer-Sicherheit. Hier erfahren Sie mehr über die verschiedenen Bedrohungen, denen Ihr Computer während einer bestehenden Internetverbindung ausgesetzt ist (Malware, Phishing, Spams, Cyber-Kriminelle).

Ständig werden neue Artikel zu den neuesten Threats, aktuellen Sicherheitstrends und anderen Informationen zur Computersicherheits-Branche eingestellt, damit Sie up-to-date bleiben.

Die Adresse von HOTforSecurity ist http://www.hotforsecurity.com.

# 36. KONTAKTINFORMATIONEN

Effiziente Kommunikation ist der Schlüssel zu einem erfolgreichen Unternehmen. BITDEFENDER hat sich seit 2001 einen herausragenden Ruf erarbeitet, indem es seine Kommunikation immer besser gemacht hat, um die Erwartungen unserer Kunden und Partner noch zu übertreffen. Für jedwede Fragen stehen wir Ihnen gerne zur Verfügung.

## 36.1. Kontaktadressen

Vertrieb: vertrieb@bitdefender.de
Support-Center:http://www.bitdefender.de/support/consumer.html
Dokumentation: documentation@bitdefender.com
Händler vor Ort:http://www.bitdefender.de/partners/
Partnerprogramm: partners@bitdefender.com
Medienkontakt: pr@bitdefender.com
Karriere: jobs@bitdefender.com
Bedrohungseinsendungen: virus_submission@bitdefender.com
Spam-Einsendungen: spam_submission@bitdefender.com
Missbrauch melden: abuse@bitdefender.com
Webseite:http://www.bitdefender.de

## 36.2. Lokale Vertriebspartner

Bitdefender-Händler stehen für vertriebliche und allgemeine Fragen und Informationen in ihren jeweiligen Regionen jederzeit zur Verfügung.

So finden Sie einen Bitdefender-Händler in Ihrem Land:

1. Gehen Sie zu http://www.bitdefender.de/partners/partner-locator.html.
2. Geben Sie über die entsprechenden Optionen Ihren Wohnort und Ihr Land an.
3. Falls Sie in Ihrem Land keinen Bitdefender-Händler finden, können Sie uns gerne unter vertrieb@bitdefender.de kontaktieren. Schreiben Sie uns Ihre E-Mail in Englisch, damit wir Ihnen umgehend helfen können.

## 36.3. Bitdefender-Niederlassungen

Bitdefender-Niederlassungen stehen Ihnen für betriebliche und allgemeine Fragen und Informationen in ihren jeweiligen Bereichen jederzeit zur

Verfügung. Die genauen Kontaktdaten und Adressen finden Sie in der unten stehenden Auflistung.

## U.S.A

**Bitdefender, LLC**
6301 NW 5th Way, Suite 4300
Fort Lauderdale, Florida 33309
Telefon (Geschäftsstelle&Vertrieb): 1-954-776-6262
Vertrieb: sales@bitdefender.com
Technischer Support: https://www.bitdefender.com/support/consumer.html
Web: https://www.bitdefender.com

## Großbritannien und Irland

**BITDEFENDER LTD**
C/O Howsons Winton House, Stoke Road, Stoke on Trent
Staffordshire, United Kindon, ST4 2RW
E-Mail: info@bitdefender.co.uk
Telefon: (+44) 2036 080 456
Vertrieb: sales@bitdefender.co.uk
Technischer Support: https://www.bitdefender.co.uk/support/
Web: https://www.bitdefender.co.uk

## Deutschland

**Bitdefender GmbH**
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Geschäftsstelle: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Vertrieb: vertrieb@bitdefender.de
Technischer Support: https://www.bitdefender.de/support/consumer.html
Web: https://www.bitdefender.de

## Dänemark

**Bitdefender APS**
Agern Alle 24, 2970 Hørsholm, Denmark
Geschäftsstelle: +45 7020 2282

Technischer Support: http://bitdefender-antivirus.dk/
Web: http://bitdefender-antivirus.dk/

## Spanien

**Bitdefender España, S.L.U.**
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Telefon: +34 902 19 07 65
Vertrieb: comercial@bitdefender.es
Technischer Support: https://www.bitdefender.es/support/consumer.html
Webseite: https://www.bitdefender.es

## Rumänien

**BITDEFENDER SRL**
Complex DV24, Building A, 24 Delea Veche Street, Sector 2
Bucharest
Fax: +40 21 2641799
Telefon Vertrieb: +40 21 2063470
Vertrieb E-Mail: sales@bitdefender.ro
Technischer Support: https://www.bitdefender.ro/support/consumer.html
Webseite: https://www.bitdefender.ro

## Vereinigte Arabische Emirate

**Dubai Internet City**
Building 17, Office # 160
Dubai, UAE
Telefon Vertrieb: 00971-4-4588935 / 00971-4-4589186
Vertrieb E-Mail: mena-sales@bitdefender.com
Technischer Support: https://www.bitdefender.com/support/consumer.html
Webseite: https://www.bitdefender.com

# Glossar

**Abonnement**

Ein Kaufvertrag, der Benutzern das Recht einräumt, ein bestimmtes Produkt oder eine Dienstleistung auf einer bestimmten Anzahl von Geräten und für einen bestimmten Zeitraum in Anspruch zu nehmen. Ein abgelaufenes Abonnement kann unter Verwendung der vom Nutzer beim Ersterwerb angegebenen Informationen automatisch verlängert werden.

**Advanced Persitent Threats**

Advanced Persistent Threat (APT) nutzen Sicherheitslücken im System, um wichtige Daten zu stehlen und an ihre Quellen zu übermitteln. Organisationen, Unternehmen und Regierungsbehörden sind eine große Zielgruppe, die von dieser Bedrohung ins Visier genommen wird.

Advanced Persistent Threats sollen so lange wie möglich unentdeckt bleiben. Während dieser Zeit sollen sie das System überwachen und wichtige Daten sammeln, ohne dabei die Zielcomputer zu beschädigen. Die Bedrohung wird durch PDF-Dateien oder Office-Dokumente in das Netzwerk eingebracht, die keinen Verdacht erregen, so dass jeder Benutzer diese Dateien ausführen kann.

**Adware**

Adware wird häufig mit einer anderen Anwendung kombiniert, die kostenlos ist, solange der Nutzer die Adware akzeptiert. Adware-Anwendungen werden in der Regel installiert, nachdem der Nutzer einer Lizenzvereinbarung zugestimmt hat. In der Lizenzvereinbarung wird auch der Zweck der Anwendung genannt, und somit liegt keine Rechtswidrigkeit vor.

Allerdings können Popup-Anzeigen mit der Zeit sehr lästig werden und in manchen Fällen die Systemperformance beeinträchtigen. Zudem kann aufgrund der Daten, die manche dieser Programme sammeln, die Privatsphäre von Nutzern verletzt werden, die sich über die Bedingungen in der Lizenzvereinbarung nicht völlig im Klaren waren.

**AktiveX**

ActiveX ist ein Programmuster, dass von anderen Programmen und Betriebssystemkomponenten unter Windows aufgerufen werden kann. Die ActiveX Technologie wird von Microsofts Internet Explorer benutzt,

damit interaktive Webseiten eher wie Programme und nicht wie statische Seiten angezeigt werden. Mit ActiveX können die Benutzer z.B. Fragen stellen oder beantworten, Buttons verwenden, oder verschiedenartige Interaktionen mit der Webseite herstellen. ActiveX-Steuerelemente werden oft in Visual Basic geschrieben.

Erwähnenswert ist, dass bei AktiveX die Sicherheitskontrollen fehlen, deshalb raten Computersicherheitsexperten davon ab, AktiveX über das Internet zu nutzen.

**Aktivierungs-Code**

Dabei handelt es sich um einen eindeutigen Schlüssel, der käuflich erworben und zur Aktivierung eines Produkts oder eines Dienstes verwendet werden kann. Mit einem Aktivierungscode kann ein gültiges Abonnement für einen bestimmten Zeitraum und eine bestimmte Anzahl an Geräten aktiviert werden. Zudem kann mit einem solchen Code eine Abonnement verlängert werden, solange es sich auf das gleiche Produkt oder den gleichen Dienst bezieht.

**Arbeitsspeicher**

Interne Speicherbereiche im Rechner. Der Begriff Arbeitsspeicher bezeichnet Datenträger in Form von sehr schnellen Chips. Dies steht im Gegensatz zu Speicherplatz, der sich auf Magnetbändern oder Datenträgern befindet. Jeder Rechner hat eine gewisse Menge Arbeitsspeicher. Dieser wird auch Hauptspeicher oder RAM bezeichnet.

**Archiv**

Ein Datenträger, ein Magnetband oder ein Ordner mit Dateien, die von einem Backup erzeugt wurden.

Eine Datei, die eine oder mehrere Dateien in einem komprimierten Format enthält.

**Backdoor (Hintertür)**

Eine Sicherheitslücke eines Systems, die der Entwickler oder Administrator absichtlich hinterlässt. Der Grund dafür muss nicht immer bösartig sein. Manche Betriebssysteme haben schon standardmäßig privilegierte Konten eingerichtet, damit diese von den Kundendienst-Technikern oder Programmierern der Hersteller benutzt werden können.

**Bedrohung**

Ein Programm oder ein Stück Code, das auf einen Rechner kopiert wird und sich allein ausführt, ohne dass es der Besitzer des Rechners will oder merkt. Die meisten Bedrohungen können sich auch selbst vervielfältigen. Alle Computerbedrohungen wurden von Menschen programmiert. Eine einfache Bedrohung, die sich immer wieder vervielfältigen kann, ist sehr einfach zu programmieren. Sogar eine solch einfache Bedrohung kann gefährlich sein, da sie im Handumdrehen sämtlichen Arbeitsspeicher belegen und so das System lahmlegen kann. Noch gefährlicher sind Bedrohungen, die sich über Netzwerke hinweg selbst weiterversenden und Sicherheitssysteme umgehen.

**Befehlszeile**

Die Befehlszeile ist eine zeichenorientierte Benutzerschnittstelle. Die Kommunikation zwischen Benutzer und Computer findet ausschließlich durch die Eingabe von bestimmten Befehlen statt, die sich aus einzelnen Buchstabenfolgen zusammensetzen. Als Eingabegerät wird eine Tastatur benutzt. Die Verwendung einer Maus ist nicht möglich. Auf der Befehlszeile werden die einzelnen Anweisungen in einer bestimmten Befehlssprache eingegeben, die vom Computer und seiner Software ausgewertet und mit den entsprechenden Ergebnissen auf dem Ausgabegerät (meistens ein Monitor) wieder an den Benutzer übergeben werden.

**Bootsektor**

Der erste Sektor einer Festplatte oder Diskette. Hier liegen Daten, die das Betriebssystem zum Booten (Starten) braucht.

**Bootvirus**

Eine Bedrohung, der den Bootsektor einer Festplatte oder eines Diskettenlaufwerks infiziert. Beim Versuch von einer Diskette, die mit einem Bootvirus infiziert ist, zu booten wird diese Bedrohung im Arbeitsspeicher aktiviert. Bei jedem Neustart wird die Bedrohung so im Arbeitsspeicher aktiviert und überträgt sich auf eingelegte Wechselmedien.

**Botnet**

Der Begriff "Botnet" setzt sich aus den Wörtern "Robot" und "Network" zusammen. Bei Botnets handelt es sich um ein Netz aus mit Bedrohungen infizierten Geräten, die mit dem Internet verbunden und für den Versand

von Spam, den Diebstahl von Daten, die Fernsteuerung von anfälligen Geräten oder die Verbreitung von Spyware, Ransomware und anderen Bedrohungsarten verwendet werden. Ziel ist es, möglichst viele mit dem Internet verbundene Geräte zu infizieren, so z. B. PCs, Server, Mobilgeräte oder IoT-Geräte in den Netzwerken großer Unternehmen oder Branchen.

**Cookie**

In der Internetbranche werden mit Cookies kleine Dateien bezeichnet, die Daten über einzelne Computer enthalten und die von den Werbetreibenden analysiert und verwendet werden, um die Interessen und Vorlieben der Benutzer herauszufinden. Die Cookie-Technologie wird stetig weiterentwickelt mit dem Ziel Benutzern nur noch solche Werbung anzuzeigen, die ihren Interessen entspricht. Für viele ist dies ein zweischneidiges Schwert. Einerseits ist es praktisch, nur Anzeigen zu sehen, an denen man interessiert ist. Anderseits bedeutet es, dass Online-Aktivitäten der Benutzer gewissermaßen auf Schritt und "Klick" verfolgt werden. Es ist also verständlich, dass in diesem Zusammenhang Datenschutz ein umstrittenes Thema ist und viele sich unwohl fühlen, quasi als SKU-Nummer (die Strichcodes auf den Packungen, die im Geschäft an der Theke gescannt werden) betrachtet zu werden. Auch wenn diese Sicht etwas extrem erscheint, ist sie doch manchmal korrekt.

**Dateierweiterung**

Der Teil hinter dem Punkt im Dateinamen. Die Erweiterung oder Extension beschreibt die Art der Daten, die in einer Datei gespeichert sind.

Viele Betriebssysteme benutzen Dateierweiterungen, z.B. Unix, VMS, MS-DOS. Sie sind gewöhnlich ein bis drei Buchstaben lange (alte Betriebssysteme können oft nicht mehr als drei Buchstaben unterstützen). Beispiele sind "exe" ausführbare Dateien, "ps" für PostScript oder "txt" für Text-Dateien.

**Download**

Kopiert Daten (gewöhnlich eine ganze Datei) von einer Hauptquelle auf ein Peripheriegerät. Der Begriff bezeichnet oft den Kopiervorgang von einem Online Service auf den eigenen Rechner. Download oder Herunterladen kann auch das Kopieren einer Datei von einem Netzwerkserver auf einen Netzwerkrechner bedeuten.

**Durchsuchen**
Kurzform für Web-Browser, ein Programm, mit dem Internetseiten aufgerufen und angezeigt werden können. Bekannte Browser sind Microsoft Internet Explorer, Mozilla Firefox und Google Chrome. Dies sind graphische Browser, was bedeutet, dass sie sowohl Grafiken als auch Texte anzeigen können. Weiterhin können die meisten Browser Multimedia-Daten wie Klang- und Videodateien anzeigen, wobei sie für diverse Formate Plug-Ins (zusätzliche Softwarekomponenten) benutzen.

**E-Mail**
Elektronische Post. Ein Dienst, der Nachrichten an andere Rechner über ein lokales oder ein globales Netzwerk übermittelt.

**E-Mail Client**
Ein E-Mail-Client ist eine Anwendung, die das Senden und Empfangen von E-Mails ermöglicht.

**Ereignisanzeige**
Ereignisse oder Erscheinungen, die in einem Programm vorkommen. Ereignisse können Benutzeraktionen, wie zum Beispiel Mausklicks oder Tastatureingaben, oder Systemereignisse, wie zum Beispiel ungenügender Speicher, sein.

**Fehlalarm**
Erscheint, wenn ein Virenscanner eine Datei als infiziert erkennt, obwohl dies nicht der Fall ist.

**Heuristik**
Eine Methode, um neue Bedrohungen zu identifizieren. Diese Scan-Methode benötigt keine konkreten Bedrohungsinformationen. Der Vorteil eines heuristischen Scans ist, dass man nicht von einer neuen Variante einer alten Bedrohung getäuscht werden kann. Manchmal kann jedoch auch ein verdächtiger Code in einem normalen Programm gemeldet werden, ein sogenannter Fehlalarm oder "falsch-positive Meldung" wird angezeigt.

**Honeypot**
Ein Computersystem, das als Köder dient, um Hacker anzulocken und danach ihr Verhalten zu beobachten. Daraus lassen sich Schlüsse ziehen, mit welchen Methoden Sie Daten sammeln. Besonders Unternehmen

und Konzerne setzen auf den Einsatz dieser "Honigtöpfe", um ihren Sicherheitslage zu verbessern.

**IP**

Internet Protocol - Das TCP/IP Protokoll ist verantwortlich für die korrekte IP Adressierung und die korrekte Zustellung der Datenpakete.

**Java Applet**

Ein Java Programm, das nur auf Webseiten läuft. Um ein Applet auf einer Webseite zu benutzen, gibt man den Namen und die Größe (Länge und Breite in Pixel) an, die das Applet einnehmen kann. Wenn die Webseite abgerufen wird, lädt der Browser das Applet vom Server herunter und führt es auf der Benutzermaschine (dem Client) aus. Applets sind keine Anwendungen, da sie von strengen Sicherheitsprotokollen gesteuert werden.

Obwohl Applets z. B. auf dem Client laufen, können diese keine Daten auf der Maschine des Clients lesen oder schreiben. Zusätzlich sind die Applets dahingehend beschränkt, dass sie nur Daten aus der Domain lesen und schreiben können, zu der sie gehören.

**Keylogger**

Ein Keylogger ist eine Anwendung, die alle Ihre Tastenanschläge aufzeichnet.

Keylogger sind an sich nicht schädlich. Sie können auch legitim eingesetzt werden, um beispielsweise die Aktivitäten von Angestellten oder Kindern zu überwachen. Sie werden jedoch zunehmend von Cyber-Kriminellen mit bösartiger Absicht eingesetzt (um beispielsweise private Daten wie Benutzernamen oder Passwörter zu sammeln).

**Komprimierte Programme**

Eine Datei in einem komprimierten Format. Viele Betriebssysteme und Anwendungen enthalten Befehle, mit denen Dateien komprimiert werden können, sodass diese weniger Speicherplatz benötigen. Zum Beispiel: Angenommen, Sie haben einen Text, der 10 aufeinander folgende Leerzeichen enthält. Normalerweise belegen diese Leerzeichen dann 10 Bytes an Speicherplatz.

Ein Programm, das Dateien komprimiert, würde die Leerzeichen durch ein Sonderzeichen „Leerzeichenreihe“ ersetzen, gefolgt von der Zahl der Leerzeichen, die ersetzt wurden. In diesem Fall sind nur noch zwei Bytes

notwendig statt zehn. Das wäre ein Beispiel für eine Komprimierungstechnik, es gibt aber noch viele andere.

**Laufwerk**

Ein Gerät, das rotierende Speichermedien lesen und beschreiben kann.

Ein Festplatten-Laufwerk liest und beschreibt Festplatten.

Ein Disketten-Laufwerk liest und beschreibt Disketten.

Laufwerke können sowohl interner (im Rechner eingebaut) als auch externer (in einem Gehäuse, das an den Rechner angeschlossen wird) Art sein.

**Logdatei (Berichtsdatei)**

Eine Datei, die stattgefundene Aktivitäten aufzeichnet. Zum Beispiel speichert Bitdefender eine Prokolldatei mit den geprüften Pfaden, Ordnern, der Anzahl der gescannten Archive und Dateien sowie der Anzahl der gefundenen infizierten oder verdächtigen Dateien.

**Makrovirus**

Eine Bedrohungsart, die in einem Dokument als eingebettetes Makro verschlüsselt wird. Viele Anwendungen, wie Microsoft Word und Excel, unterstützen leistungsstarke Makrosprachen.

Diese Anwendungen ermöglichen das Einbetten eines Makros in ein Dokument, welches dann bei jedem Öffnen des Dokuments ausgeführt wird.Ein Makro ist eine Aufzeichnung des Ablaufs von Routineaufgaben innerhalb des makrofähigen Programms, das dann immer wieder verwendet werden kann.

**Nicht heuristisch**

Diese Scan-Methode benötigt konkrete Bedrohungsinformationen. Der Vorteil eines nicht-heuristischen Scans ist, dass er nicht von einer Scheinbedrohung getäuscht werden kann und so Fehlalarme verhindert.

**Pfad**

Zeigt die Stelle an, an der sich eine Datei in einem Rechner befindet. Diese Pfadangaben enthalten gewöhnlich den hierarchischen Aufbau des Dateiverzeichnisses: Laufwerke, Ordner, Unterverzeichnisse, die Datei und ihre Erweiterung.

Der Weg zwischen zwei Punkten, wie zum Beispiel der Kommunikationskanal zwischen zwei Rechnern.

**Phishing**

Das Senden einer E-Mail an einen Benutzer, in der der Sender sich als Vertreter eines legitimen Unternehmens ausgibt und versucht, den Empfänger so zu manipulieren, dass er persönliche Informationen preisgibt, die dann zum Diebstahl der Identität verwendet werden können. Die E-Mail leitet den Benutzer dann auf eine Webseite, auf der er aufgefordert wird, vertrauliche Daten wie Kreditkartennummern, TANs oder PINs preiszugeben. Es wird oft vorgegeben, dass dies aus Gründen der Aktualisierung geschehen soll. Diese Webseiten sind jedoch gefälscht und wurden eigens für den Diebstahl dieser Daten eingerichtet.

**Photon**

Photon ist eine innovative und unaufdringliche Bitdefender-Technologie, die eigens entwickelt wurde, um die Auswirkungen der Sicherheitslösung auf die Systemleistung zu minimieren. Durch die Hintergrundüberwachung aller PC-Aktivitäten werden Nutzungsprofile erstellt, mit denen Start- und Scan-Prozesse optimiert werden können.

**Polymorpher Virus**

Eine Bedrohung, die ihre Form mit jeder Datei, die sie infiziert, ändert. Da diese Bedrohungen kein beständiges binäres Muster haben, sind sie sehr schwer zu erkennen.

**Ransomware**

Bei Ransomware handelt es sich um schädliche Programme, die anfällige Systeme für den Benutzer sperren und für deren Freigabe Lösegeld erpressen. CryptoLocker, CryptoWall und TeslaWall sind nur einige Beispiele für Ransomware, die es auf Benutzercomputer abgesehen haben.

Die Infektion kann sich durch das Aufrufen eine Spam-Nachricht, das Herunterladen eines E-Mail-Anhangs oder die Installation von Anwendungen ausbreiten, ohne dass der Benutzer es überhaupt bemerkt. Ransomware-Hacker nehmen herkömmliche Benutzer und Unternehmen ins Visier.

**Rootkit**

Bei einem Rootkit handelt es sich um eine Sammlung von Software-Tools, mit denen auf ein System mit Administratorrechten zugegriffen werden kann. Der Begriff wurde ursprünglich nur für UNIX-Systeme verwendet und beschrieb rekompilierte Tools, mit denen sich Angreifer Administratorrechte verschaffen und so ihre Anwesenheit vor den tatsächlichen Administratoren verbergen konnten.

Die Hauptaufgabe eines Rootkits besteht darin, Prozesse, Dateien und Protokolle zu verstecken. Sie können auch Daten von Terminals, Netzwerkverbindungen oder Peripheriegeräten abfangen, falls Sie eine entsprechende Software eingebaut haben.

Rootkits sind nicht grundsätzlich schädlich. Einige Systeme und Anwendungen verstecken z. B. wichtige Dateien mithilfe von Rootkits. Sie werden jedoch oft dazu missbraucht, Bedrohungen zu verbergen oder unbemerkt einen Eindringling einzuschleusen. In Kombination mit anderen Bedrohungen stellen Rootkits eine große Gefahr für Ihr System dar. Denn sie können den Datenverkehr abhören, Sicherheitslücken in Ihrem System schaffen, Dateien und Zugangsdaten verändern, und das alles, ohne entdeckt zu werden.

**Schnittstelle**

Stelle eines Rechners, an die ein Gerät angeschlossen werden kann. Rechner haben verschiedenartige Schnittstellen. Im Inneren gibt es Schnittstellen zum Anschluss von Festplatten, Grafikkarten und Tastaturen. Extern haben Rechner Schnittstellen zum Anschluss von Modems, Druckern und anderen Peripheriegeräten.

In TCP/IP und UDP Netzwerken, ein Endpunkt zu logischen Verbindungen. Die Schnittstellennummer gibt die Art der Schnittstelle an. Zum Beispiel, Schnittstelle 80 wird für HTTP Traffic verwendet.

**Script**

Ein anderer Begriff für Makro- oder Batchdatei. Ein Skript ist eine Befehlsliste, die ohne Benutzereingriff ausgeführt werden kann.

**Spam**

Junk-E-Mail oder Junk-Postings in Newsgroups. Im Allgemeinen versteht man darunter jede Art von unerwünschter E-Mail.

**Spyware**

Software, die unentdeckt vom Nutzer private und geheime Anwenderdaten über seine Internetverbindung abgreift. Dies geschieht in der Regel zu Werbezwecken. Typischerweise sind Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Shareware-Programmen enthalten, die aus dem Internet heruntergeladen werden können. Die große Mehrzahl von Shareware- und Freeware-Anwendungen ist natürlich frei von Spyware. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an einen Dritten. Spyware kann auch Informationen über E-Mail-Adressen und sogar Passwörter und Kreditkartennummern sammeln.

Einer Bedrohung durch ein trojanisches Pferd ähnelt Spyware darin, dass die Anwender das Produkt unwissentlich gemeinsam mit etwas anderem installieren. Opfer von Spyware wird man oft dann, wenn man sich bestimmte Peer-to-Peer-Dateiaustauschprogramme herunterlädt.

Ganz abgesehen von den Fragen der Ethik und des Datenschutzes belegt Spyware auch unnötig Systemressourcen und Bandbreite, indem über die Internetverbindung des Nutzers Informationen an den Spyware-Heimatserver gesendet werden. Da Spyware Speicher und Systemressourcen verbraucht, können die im Hintergrund laufenden Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.

**Startup Objekt (Autostart-Objekt)**

Jede Datei, die sich in diesem Ordner befindet, wird geöffnet, wenn der Rechner gestartet wird. Das können z. B. ein Startbildschirm, eine Sounddatei, die beim Systemstart abgespielt wird, ein Erinnerungskalender oder auch Apps sein. Gewöhnlich wird eine Alias-Datei (Verknüpfung) statt der eigentlichen Datei in diesen Ordner gelegt.

**Symbolleiste**

Die Symbolleiste wurde mit Windows 95 eingeführt und befindet sich auf der Windows Task-Leiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet). Sie enthält kleine Symbole zur Information und zum leichteren Zugriff auf Systemfunktionen wie Drucker, Modems, Lautstärke und anderes. Um auf die Details und Optionen dieser

Funktionen zuzugreifen, ist ein Doppelklick oder ein Klick mit der rechten Maustaste erforderlich.

**TCP/IP**

Transmission Control Protocol/Internet Protocol – im Internet weit verbreiteter Netzwerkprotokollsatz, der die Kommunikation zwischen verbundenen Computernetzwerken mit verschiedenen Hardware-Architekturen und Betriebssystemen ermöglicht. TCP/IP bietet eine Möglichkeit, all diese unterschiedlichen Komponenten zu Kommunikationszwecken miteinander zu verbinden.

**Trojaner**

Ein bösartiges Programm, das sich als eine legitime Anwendung ausgibt. Anders als Schad-Software und Würmer vervielfältigen sich Trojaner nicht selbst, können aber dennoch großen Schaden anrichten. Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Bedrohungen zu befreien, stattdessen aber den Rechner infiziert.

Der Begriff entstammt einer Geschichte in Homers "Ilias", in der die Griechen ihren Feinden, den Trojanern, angeblich als Sühnegabe ein riesiges hölzernes Pferd schenkten. Aber nachdem die Trojaner das Pferd in die Stadt gebracht hatten, schlichen sich die im Bauch des hölzernen Pferdes versteckten Soldaten bei Nacht heraus, öffneten die Tore der Stadt und ermöglichten somit ihren Landsleuten, in die Stadt einzudringen und auf diese Weise Troja zu besetzen.

**Update (Aktualisierung)**

Eine neue Software- oder Hardwareversion, die eine ältere Version desselben Produkts ersetzt. Die Update-Installationsroutine eines Programms prüft oft, ob eine ältere Versionen auf dem Rechner installiert ist, da sonst kein Update installiert werden kann.

Bitdefender verfügt über eine eigene Update-Funktion, über die Sie manuell nach Updates suchen oder das Produkt automatisch aktualisieren lassen können.

**Update der Bedrohungsinformationen**

Das binäre Muster einer Bedrohung, wird von der Sicherheitslösung zur Erkennung und Beseitigung einer Bedrohung genutzt.

**Virtual Private Network (VPN)**

Mit dieser Technologie ist es möglich, eine zeitlich begrenzte und verschlüsselte direkte Verbindung mit einem bestimmten Netzwerk auch über ein weniger gut gesichertes Netzwerk aufzubauen. Auf diese Weise können Daten sicher und verschlüsselt versandt und empfangen werden und sind für neugierige Augen nur schwer einsehbar. Bei einem Sicherheitsnachweis handelt es sich um eine Authentifizierung, die ausschließlich über einen Benutzernamen und ein Passwort erfolgen kann.

**Wurm**

Ein Programm, das sich selbst kopiert und über ein Netzwerk verbreitet. Es kann sich nicht an andere Programme anhängen.