

Bitdefender® ANTIVIRUS PLUS 2018



BENUTZERHANDBUCH



Bitdefender Antivirus Plus 2018 **Benutzerhandbuch**

Veröffentlicht 25.05.2018

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.



Inhaltsverzeichnis

Installation	1
1. Vor der Installation	2
2. Systemanforderungen	3
2.1. Mindestsystemanforderungen	3
2.2. Empfohlene Systemanforderungen	3
2.3. Software-Anforderungen	4
3. Installieren Ihres Bitdefender-Produkts	5
3.1. Über Bitdefender Central installieren	5
3.2. Installation vom Installationsdatenträger	7
Inbetriebnahme	13
4. Grundlagen	14
4.1. Das Bitdefender-Fenster öffnen	15
4.2. Probleme beheben	16
4.2.1. Assistent für Sicherheitsprobleme	16
4.2.2. Konfigurieren von Statusbenachrichtigungen	17
4.3. Benachrichtigungen	18
4.4. Autopilot	19
4.5. Profile	20
4.5.1. Automatische Aktivierung von Profilen konfigurieren	21
4.6. Passwortschutz für Bitdefender-Einstellungen	21
4.7. Anonyme Nutzungsberichte	22
4.8. Benachrichtigungen zu Sonderangeboten	22
5. Bitdefender-Benutzeroberfläche	24
5.1. Task-Leisten-Symbol	24
5.2. Hauptfenster	26
5.2.1. Statusbereich	26
5.2.2. Linker Seitenbereich	27
5.2.3. Schaltflächen und Zugriff auf die Funktionen	28
5.2.4. Fußleiste	29
5.3. Die Bitdefender-Bereiche	29
5.3.1. Schutz	30
5.3.2. Privatsphäre	31
5.4. Sicherheits-Widget	32
5.4.1. Dateien und Verzeichnis scannen	33
5.4.2. Das Sicherheits-Widget ausblenden/anzeigen	34
5.5. Aktivität	34
5.5.1. Aufrufen des Sicherheitsberichts	36
5.5.2. Aktivieren oder Deaktivieren der Benachrichtigungen zum Sicherheitsbericht	37
6. Bitdefender Central	38
6.1. So können Sie Bitdefender Central aufrufen:	38



6.2. Meine Abonnements	39
6.2.1. Verfügbare Abonnements anzeigen	39
6.2.2. Ein neues Gerät hinzufügen	39
6.2.3. Abonnement verlängern	40
6.2.4. Abonnement aktivieren	40
6.3. Meine Geräte	41
6.4. Mein Konto	43
6.5. Benachrichtigungen	43
7. Bitdefender auf dem neuesten Stand halten	44
7.1. Überprüfen, ob Bitdefender auf dem neuesten Stand ist	45
7.2. Durchführung eines Updates	45
7.3. Aktivieren / Deaktivieren der automatischen Updates	46
7.4. Update-Einstellungen anpassen	46
7.5. Regelmäßige Updates	48

Gewusst wie **49**

8. Installation	50
8.1. Wie installiere ich Bitdefender auf einem zweiten Computer?	50
8.2. Wie kann ich Bitdefender neu installieren?	50
8.3. Wo kann ich mein Bitdefender-Produkt herunterladen?	52
8.4. Wie kann ich die Sprache für mein Bitdefender ändern?	52
8.5. Wie verfare ich mit meinem Bitdefender-Abonnement nach einem Windows-Upgrade?	54
8.6. Wie kann ich ein Upgrade auf die neueste Bitdefender-Version durchführen? ..	57
9. Abonnements	58
9.1. Wie kann ich mein Bitdefender-Abonnement mithilfe eines Lizenzschlüssels aktivieren?	58
10. Bitdefender Central	60
10.1. Wie melde ich mit einem anderen Benutzerkonto bei Bitdefender Central an?	60
10.2. Wie kann ich die Bitdefender Central-Hilfemeldungen deaktivieren?	60
10.3. Ich habe das Passwort vergessen, das ich für mein Bitdefender-Konto festgelegt habe. Wie kann ich es zurücksetzen?	61
10.4. Wie kann ich die Benutzersitzungen in meinem Bitdefender-Konto verwalten?	62
11. Prüfen mit Bitdefender	63
11.1. Wie kann ich eine Datei oder einen Ordner scannen?	63
11.2. Wie scanne ich mein System?	63
11.3. Wie plane ich einen Scan?	64
11.4. Wie kann ich eine benutzerdefinierte Scan-Aufgabe anlegen?	64
11.5. Wie kann ich einen Ordner vom Scan ausnehmen?	65
11.6. Wie gehe ich vor, wenn Bitdefender eine saubere Datei als infiziert eingestuft hat?	66
11.7. Wo sehe ich, welche Bedrohungen Bitdefender gefunden hat?	67
12. Privatshpäreschutz	69



12.1. Wie sichere ich meine Online-Transaktionen ab?	69
12.2. Wie lösche ich mit Bitdefender eine Datei unwiderruflich?	69
13. Nützliche Informationen	71
13.1. Wie kann ich meine Sicherheitslösung selbst testen?	71
13.2. Wie kann ich Bitdefender entfernen?	71
13.3. Wie kann ich Bitdefender VPN entfernen?	72
13.4. Wie fahre ich den Computer automatisch herunter, nachdem der Scan beendet wurde?	73
13.5. Wie konfiguriere ich Bitdefender für die Nutzung einer Proxy-Verbindung?	74
13.6. Ist auf meinem System die 32- oder 64-Bit-Version von Windows installiert?	76
13.7. Wie kann ich in Windows versteckte Objekte anzeigen?	76
13.8. Wie entferne ich andere Sicherheitslösungen?	77
13.9. Wie führe ich einen Neustart im abgesicherten Modus durch?	79

Die Sicherheitselemente im Detail 81

14. Virenschutz	82
14.1. Zugriff-Scans (Echtzeitschutz)	83
14.1.1. Aktivieren / Deaktivieren des Echtzeitschutzes	83
14.1.2. Erweiterte Einstellungen des Echtzeitschutzes konfigurieren	84
14.1.3. Wiederherstellen der Standardeinstellungen	88
14.2. Bedarf-Scan	88
14.2.1. Eine Datei oder einen Ordner auf Bedrohungen prüfen	89
14.2.2. Durchführen von Quick Scans	89
14.2.3. Durchführen von System-Scans	90
14.2.4. Benutzerdefinierte Scans durchführen	91
14.2.5. Viren-Scan-Assistent	94
14.2.6. Scan-Protokolle lesen	97
14.3. Automatischer Scan von Wechselmedien	98
14.3.1. Wie funktioniert es?	99
14.3.2. Verwalten des Scans für Wechselmedien	100
14.4. Host-Datei scannen	100
14.5. Konfiguration der Scan-Ausschlüsse	101
14.5.1. Dateien und Ordner vom Scan ausschließen	101
14.5.2. Dateiendungen vom Scan ausschließen	102
14.5.3. Verwalten von Scan-Ausschlüssen	103
14.6. Verwalten von Dateien in Quarantäne	104
15. Erweiterte Gefahrenabwehr	106
15.1. Aktivieren oder Deaktivieren der Advanced Threat Defense	106
15.2. Anzeigen von erkannten Ransomware-Angriffen	106
15.3. Erkannte verdächtige Apps anzeigen	107
15.4. Hinzufügen von Prozessen zu den Ausschlüssen	107
16. Internet-Schutz	109
16.1. Bitdefender-Benachrichtigungen im Browser	111
17. Schwachstellen	112
17.1. Scannen des Computers nach Schwachstellen	112



17.2. Automatische Schwachstellensuche	114
17.3. WLAN-Sicherheitsberater	116
17.3.1. Aktivieren und Deaktivieren der Benachrichtigungen des WLAN-Sicherheitsberaters	117
17.3.2. Konfiguration Ihres Heim-WLANs	117
17.3.3. Öffentliches WLAN	118
17.3.4. Abrufen von Informationen zu WLAN-Netzwerken	118
18. Sichere Dateien	120
18.1. Aktivieren und Deaktivieren von Sichere Dateien	120
18.2. Schützen Sie Ihre persönlichen Dateien vor Ransomware-Angriffen	121
18.3. Konfiguration des App-Zugriffs	122
18.4. Schutz beim Systemstart	122
19. Passwortmanager-Schutz für Ihre Anmeldedaten	124
19.1. Neue Geldbörsen-Datenbank erstellen	125
19.2. Bestehende Datenbank importieren	125
19.3. Die Geldbörse-Datenbank exportieren	126
19.4. Synchronisieren Ihrer Geldbörsen in der Cloud	127
19.5. Geldbörse-Anmeldedaten verwalten	127
19.6. Aktivieren oder Deaktivieren des Passwortmanager-Schutzes	128
19.7. Verwaltung der Passwortmanager-Einstellungen	128
20. VPN	132
20.1. VPN installieren	132
20.2. Öffnen des VPN	133
20.3. VPN-Benutzeroberfläche	133
20.4. Abonnements	134
21. Sichere Online-Transaktionen mit Safepay	136
21.1. Bitdefender Safepay™ verwenden	137
21.2. Einstellungen verändern	138
21.3. Lesezeichen verwalten	140
22. Datenschutz	141
22.1. Endgültiges Löschen von Dateien	141
23. USB Immunizer	143
Systemoptimierung	144
24. Profile	145
24.1. Arbeitsprofil	146
24.2. Filmprofil	147
24.3. Spielprofil	149
24.4. Öffentliches WLAN-Profil	150
24.5. Akkubetriebsprofil	150
24.6. Echtzeitoptimierung	152
Problemlösung	153
25. Verbreitete Probleme beheben	154



25.1. Mein System scheint langsamer zu sein	154
25.2. Der Scan startet nicht	156
25.3. Ich kann eine App nicht mehr verwenden	158
25.4. Wie gehe ich vor, wenn Bitdefender eine sichere Website oder Online-Anwendung blockiert?	159
25.5. Wie gehe ich vor, wenn Bitdefender eine sichere Anwendung als Ransomware einstuft?	160
25.6. Wie man Bitdefender-Updates auch mit einer langsamen Internet-Verbindung durchführen kann	161
25.7. Bitdefender-Dienste antworten nicht	161
25.8. Das automatische Einfügen funktioniert bei meiner Geldbörse nicht	162
25.9. Entfernen von Bitdefender ist fehlgeschlagen	163
25.10. Mein System fährt nach der Installation von Bitdefender nicht mehr hoch ..	164
26. Entfernung von Bedrohungen	168
26.1. Bitdefender-Rettungsmodus (Rettungsumgebung unter Windows 10)	168
26.2. Wie gehe ich vor, wenn Bitdefender eine Bedrohung auf meinem Computer findet?	173
26.3. Wie entferne ich eine Bedrohung aus einem Archiv?	174
26.4. Wie entferne ich eine Bedrohung aus einem E-Mail-Archiv?	175
26.5. Wie gehe ich vor, wenn ich eine Datei für gefährlich halte?	177
26.6. Wobei handelt es sich bei den passwortgeschützten Dateien im Scan-Protokoll?	177
26.7. Wobei handelt es sich bei den übersprungenen Objekten im Scan-Protokoll?	178
26.8. Wobei handelt es sich bei den zu stark komprimierten Dateien im Scan-Protokoll?	178
26.9. Warum hat Bitdefender ein infizierte Datei automatisch gelöscht?	178
Kontaktieren Sie uns	179
27. Hilfe anfordern	180
28. Online-Ressourcen	183
28.1. Bitdefender-Support-Center	183
28.2. Bitdefender Support-Forum	184
28.3. Das Portal HOTforSecurity	184
29. Kontaktinformationen	185
29.1. Kontaktadressen	185
29.2. Lokale Vertriebspartner	185
29.3. Bitdefender-Niederlassungen	185
Glossar	188



INSTALLATION



1. VOR DER INSTALLATION

Bevor Sie Bitdefender Antivirus Plus 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 installiert werden. Wird die Systemkonfiguration nachträglich verändert, kann es zu Leistungseinbußen und Stabilitätsproblemen kommen. Eine vollständige Liste der Systemanforderungen finden Sie im Kapitel „*Systemanforderungen*“ (S. 3).
- 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.
- 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.



2. SYSTEMANFORDERUNGEN

Sie können Bitdefender Antivirus Plus 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.

2.1. Mindestsystemanforderungen

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

2.2. 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)



2.3. 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



3. INSTALLIEREN IHRES BITDEFENDER-PRODUKTS

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

Wenn Sie eine Lizenz für mehr als einen Computer haben, (weil Sie z. B. Bitdefender Antivirus Plus 2018 für 3 PCs gekauft haben), wiederholen Sie den Installationsvorgang und aktivieren Sie Ihr Produkt mit demselben Benutzerkonto auf jedem der Computer. Dabei müssen Sie das Benutzerkonto verwenden, das Ihr aktives Bitdefender-Abonnement enthält.

3.1. 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 Antivirus Plus 2018 aktiviert.

So können Sie Bitdefender Antivirus Plus 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 Antivirus Plus 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 Antivirus Plus 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 Antivirus Plus 2018 nutzen dürfen.

Sollten Sie diesen Nutzungsbedingungen nicht zustimmen, schließen Sie das Fenster. Der Installationsprozess wird abgebrochen und 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. 90).

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 Antivirus Plus 2018-Benutzeroberfläche aufzurufen.

3.2. 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 Antivirus Plus 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 Antivirus Plus 2018 nutzen dürfen.

Sollten Sie diesen Nutzungsbedingungen nicht zustimmen, schließen Sie das Fenster. Der Installationsprozess wird abgebrochen und 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. 90).

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 im Kapitel „*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 vorausgegangenen 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 Antivirus Plus 2018-Benutzeroberfläche aufzurufen.



INBETRIEBNAHME



4. GRUNDLAGEN

Nach der Installation von Bitdefender Antivirus Plus 2018 ist Ihr Computer vor allen Arten von Bedrohungen geschützt (so z. B. vor Malware, Spyware, Ransomware, Exploits, Botnets und Trojanern).

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 mit 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 abzuwarten, 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. 132)-App installieren.

Behalten Sie den Überblick über Ihre Passwörter und Online-Konten, indem Sie sie „*Passwortmanager-Schutz für Ihre Anmeldedaten*“ (S. 124) in einer Geldbörse sicher verwahren. Mit nur einem Masterpasswort können Sie Ihre Privatsphäre vor Eindringlingen schützen, die es auf Ihr Geld abgesehen haben.

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. 116).

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. 120).

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. 145).



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 im Kapitel „*Benachrichtigungen*“ (S. 18).

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 Antivirus Plus 2018 zu nutzen und Ihre Abonnements und Geräte zu verwalten. Weitere Informationen finden Sie im Kapitel „*Bitdefender Central*“ (S. 38).

Im Abschnitt „*Gewusst wie*“ (S. 49) 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. 154) Lösungen zu den häufigsten Problemen.

4.1. Das Bitdefender-Fenster öffnen

Um das Bitdefender Antivirus Plus 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 Antivirus Plus 2018**. Noch schneller geht es mit einem Doppelklick auf das Bitdefender-Symbol **B** 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 **B**-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 **B**-Symbol in der Taskleiste möglich.

Weitere Informationen zum Bitdefender-Fenster und zum Symbol in der Task-Leiste finden Sie im Kapitel „*Bitdefender-Benutzeroberfläche*“ (S. 24).


4.2. 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.

4.2.1. 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.


4.2.2. Konfigurieren von Statusbenachrichtigungen

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

- Virenschutz
- 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.

4.3. Benachrichtigungen

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 Kurznfos 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.

4.4. Autopilot


Für alle Benutzer, die nichts weiter von Ihrer Sicherheitslösung erwarten, als zuverlässigen Schutz, ohne bei der Arbeit gestört zu werden, bietet Bitdefender Antivirus Plus 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.
- 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**.

4.5. 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-Profil 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.



4.5.1. 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. 145)

4.6. 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.

4.7. 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.

4.8. 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.



5. BITDEFENDER-BENUTZEROBERFLÄCHE

Bitdefender Antivirus Plus 2018 entspricht den Bedürfnissen sowohl von Profis als auch von Beginners. 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.

5.1. Task-Leisten-Symbol


Um das gesamte Produkt schneller zu verwalten, können Sie das Bitdefender-Symbol **B** 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**.

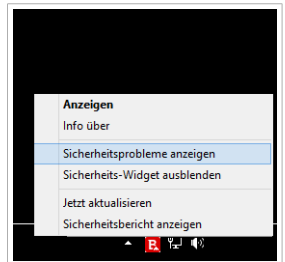
- In **Windows 10**:



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.

- **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 im Kapitel „*Probleme beheben*“ (S. 16).
- **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.



Tray Icon

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.



- F** Die Sicherheit Ihres Systems wird durch nicht-kritische Probleme beeinträchtigt. Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben.
- B** Der Bitdefender-Autopilot ist aktiviert.

Wenn Bitdefender nicht aktiv ist, ist das Symbol in der Task-Leiste grau hinterlegt: **B**. 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.

5.2. 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 eine Reihe von Aufgaben durchführen, damit Ihr System geschützt bleibt. 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.

5.2.1. 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 im Kapitel *„Probleme beheben“* (S. 16).

- 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. 19).
- 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. 44).
- Unter **Aktives Profil** sehen Sie das derzeit in Ihrem Bitdefender-Produkt aktivierte Profil. Weitere Einzelheiten finden Sie im Kapitel *„Profile“* (S. 145).

5.2.2. 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 geschredderte Dateien eingeblendet. Klicken Sie auf den Link **FUNKTIONEN ANZEIGEN**, um den Konfigurationsbereich aufzurufen.
- **📈 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 Antivirus Plus 2018 benötigen.

5.2.3. 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 zwei Bereiche im Seitenbereich links auswählen: **Schutz** und **Privatsphäre**.

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.

5.2.4. 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 Antivirus Plus 2018 auf Windows-Geräten.
- Bitdefender Antivirus for Mac auf macOS-Geräten.
- Bitdefender Mobile Security auf Android-basierten Geräten.
- Bitdefender Mobile Security auf iOS-Geräten.

5.3. Die Bitdefender-Bereiche

Das Bitdefender-Produkt besteht aus drei Bereichen, die in nützliche Funktionen unterteilt sind. So sind Sie bei der Arbeit, beim Surfen im Internet, beim Spielen oder bei der Abwicklung von Online-Zahlungen jederzeit geschützt.

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

5.3.1. Schutz

Im Bereich Schutz können Sie erweiterte Sicherheitseinstellungen vornehmen, 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. 82).

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. 109).

ERWEITERTE GEFAHRENABWEHR

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 „*Erweiterte Gefahrenabwehr*“ (S. 106).

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. 112).

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. 120).

5.3.2. Privatsphäre

Sie können die Bitdefender-VPN-App im Bereich Privatsphäre öffnen, um Ihre Online-Transaktionen zu schützen und Ihr Surf-Vergnügen abzusichern.

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 im Kapitel „*VPN*“ (S. 132).



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. 124).

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. 136).

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. 141).

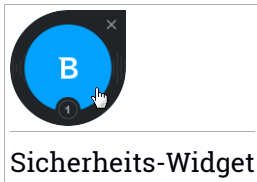
5.4. Sicherheits-Widget

Das **Sicherheits-Widget** ist die bequemste und schnellste Art Bitdefender Antivirus Plus 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-Aktivität 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 Problemlösungsassistenten 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  aussieht, um das Benachrichtigungsfenster zu öffnen. Weitere Informationen finden Sie im Kapitel „*Benachrichtigungen*“ (S. 18).

5.4.1. 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.

5.4.2. 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.

5.5. 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.



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 zwei 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. 82).

- **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. 109)

- **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. 112).

- **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 zum detaillierten Ereignisprotokoll aller Aktivitäten auf Ihrem Computer finden Sie im Kapitel *„Benachrichtigungen“* (S. 18).

- **Optimierung** - Hier erhalten Sie Informationen zu gewonnenen Speicherplatz, optimierten Anwendungen und der Akkulaufzeit, die Sie durch den Akkubetrieb gewonnen haben.

- **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. 150).

- **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. 145).

5.5.1. 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.

5.5.2. 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.




6. 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 Antivirus Plus 2018
 - Bitdefender Antivirus for Mac
 - Bitdefender Mobile Security für Android
 - Bitdefender Mobile Security for iOS
- Verwaltung und Verlängerung Ihrer Bitdefender-Abonnements.
- Neue Geräte zu Ihrem Netzwerk hinzufügen und diese Geräte aus der Ferne verwalten.

6.1. 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.

6.2. Meine Abonnements

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

6.2.1. 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.

6.2.2. Ein neues Gerät hinzufügen

Falls Ihr Abonnement mehr als ein Gerät umfasst, können Sie ein neues Gerät hinzufügen und darauf Ihr Bitdefender Antivirus Plus 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.

6.2.3. 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.

6.2.4. 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 Aktivierungscode 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.

6.3. 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 klicken 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. 90) und „*Durchführen von Quick Scans*“ (S. 89).



- **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 im Kapitel „*Schwachstellen*“ (S. 112).


6.4. Mein Konto

Im Bereich **Mein Konto** können Sie Ihr Profil anpassen, Ihr Passwort ändern sowie die Benutzersitzungen und die Hilfefmeldungen 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 Hilfefmeldungen von Bitdefender Central ein- und ausschalten und einstellen, ob Sie benachrichtigt werden möchten, wenn mit Ihren Android-Geräten Fotos gemacht werden.

6.5. Benachrichtigungen

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.



7. 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. 74) 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. 161).
- Falls Sie sich per Einwahl mit dem Internet verbinden, ist es sinnvoll, regelmäßig ein manuelles Bitdefender-Update durchzuführen. Weitere Informationen finden Sie im Kapitel *„Durchführung eines Updates“* (S. 45).



7.1. Überprüfen, ob Bitdefender auf dem neuesten Stand ist

Links im Statusbereich wird unter **Sicherheitsstatus** 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.

7.2. 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**.

7.3. 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. Eine 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.


7.4. 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.

7.5. 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.



GEWUSST WIE



8. INSTALLATION

8.1. 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. Klicken 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.

8.2. 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 Antivirus Plus 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 Antivirus Plus 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 Antivirus Plus 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.



8.3. 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.


8.4. 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 Antivirus Plus 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 Antivirus Plus 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 Antivirus Plus 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.

8.5. Wie verfare 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 Antivirus Plus 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 Antivirus Plus 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 Antivirus Plus 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 „*Installieren Ihres Bitdefender-Produkts*“ (S. 5).

8.6. 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 Upgradeinformation 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.



9. ABONNEMENTS

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

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

● Im Falle eines Upgrades auf die neueste Bitdefender-Version:

1. Nach Abschluss des Bitdefender Antivirus Plus 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 Antivirus Plus 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.




10. BITDEFENDER CENTRAL

10.1. 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 -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. 180) beschrieben mit dem Bitdefender-Support in Verbindung setzen.

10.2. 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**.



10.3. 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.



10.4. 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.



11. PRÜFEN MIT BITDEFENDER

11.1. 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.

11.2. Wie scanne ich mein System?

So können Sie einen vollständigen System-Scan durchführen:

1. Klicken Sie im linken Seitenbereich der **Bitdefender-Benutzeroberfläche** auf das **B**-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 im Kapitel „*Viren-Scan-Assistent*“ (S. 94).



11.3. 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 **B**-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.

11.4. Wie kann ich eine benutzerdefinierte Scan-Aufgabe anlegen?

Wenn Sie bestimmte Bereiche Ihres Computers scannen oder die Scan-Optionen konfigurieren möchten, können Sie eine 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 **B**-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.

11.5. Wie kann ich einen Ordner vom Scan ausnehmen?

Mit Bitdefender können Sie bestimmte Dateien, Ordner oder Dateierweiterungen 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 **B**-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.


11.6. 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 **B**-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. 76).
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. Setzen 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. 180).

11.7. 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**.





12. PRIVATSHPÄRESCHUTZ

12.1. 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.

12.2. 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.



13. NÜTZLICHE INFORMATIONEN

13.1. 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. 180) beschrieben an Bitdefender zu wenden.

13.2. Wie kann ich Bitdefender entfernen?

So können Sie Ihr Bitdefender Antivirus Plus 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 Antivirus Plus 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 Antivirus Plus 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 Antivirus Plus 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.

13.3. 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.

13.4. 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 im Kapitel „*Viren-Scan-Assistent*“ (S. 94).

13.5. 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 aktualisiert



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.



13.6. 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.

13.7. 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**.

13.8. 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 Antivirus Plus 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.



13.9. 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.



DIE SICHERHEITSELEMENTE IM DETAIL



14. 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 im Kapitel „*Automatischer Scan von Wechselmedien*“ (S. 98).

Erfahrene Benutzer können Scan-Ausschlüsse konfigurieren, wenn Sie nicht möchten, dass bestimmte Dateien oder Dateitypen gescannt werden. Weitere Informationen finden Sie im Kapitel „*Konfiguration der Scan-Ausschlüsse*“ (S. 101).

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 im Kapitel „*Verwalten von Dateien in Quarantäne*“ (S. 104).





Wenn Ihr Computer durch Bedrohungen infiziert wurde, siehe „*Entfernung von Bedrohungen*“ (S. 168). 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. 168). 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.

14.1. Zugriff-Scans (Echtzeitschutz)

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

14.1.1. 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.



14.1.2. 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 können 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; xlsn; 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 infizierte 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 gefundenen Bedrohungsinformation 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 im Kapitel *„Verwalten von Dateien in Quarantäne“* (S. 104).



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 im Kapitel „*Verwalten von Dateien in Quarantäne*“ (S. 104).



Zugriff verweigern

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

14.1.3. Wiederherstellen der Standardeinstellungen

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

Um die vorgegebenen Echtzeitschutz-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.

14.2. 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.


14.2.1. 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.


14.2.2. 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.

14.2.3. 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 im Kapitel „*Bitdefender auf dem neuesten Stand halten*“ (S. 44).
- 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 im Kapitel „*Benutzerdefinierte Scans durchführen*“ (S. 91).

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.

14.2.4. 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 **B**-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 können 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; mpv; 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; 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 infizierte 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.

14.2.5. 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 **B** 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 gefundenen Bedrohungsinformation 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 im Kapitel *„Verwalten von Dateien in Quarantäne“* (S. 104).



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. 168).

14.2.6. 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**.

14.3. 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.



14.3.1. 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. 168).

14.3.2. 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 Entdeckungsraten 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 standardisiert, sie können daher nicht geändert werden.

14.4. 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.

14.5. Konfiguration der Scan-Ausschlüsse

Mit Bitdefender können Sie bestimmte Dateien, Ordner oder Dateierendungen 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**.

14.5.1. 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**.

14.5.2. 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 Vorsicht 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**.

14.5.3. 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**.


14.6. 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 Quarantäneinstellungen 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**.



15. ERWEITERTE GEFAHRENABWEHR


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 einzelne dieser Aktionen erhält einen Wert, und jeder Prozess erhält so einen aggregierten Gesamtwert.

Als zusätzliche Sicherheitsmaßnahme erhalten Sie eine Benachrichtigung über jeden erkannten und blockierten Ransomware-Angriff, auch dann, wenn der Autopilot aktiviert ist.

15.1. 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.

15.2. 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.

15.3. 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 **B**-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.


15.4. 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 **B**-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.





16. 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 analysiert 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.



16.1. 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.



17. 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.

17.1. 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.



17.2. 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.

17.3. 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 von **Bitdefender VPN** vor.

Der Bitdefender-WLAN-Sicherheitsberater liefert Informationen zu:



- **Heim-WLAN-Netzwerken**



● Öffentlichen WLAN-Netzwerken


17.3.1. 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.

17.3.2. 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**.




17.3.3. Öffentliches WLAN

Bei Verbindungen mit einem ungesicherten oder unsicheren WLAN-Netzwerk wird das Öffentliche WiFi-Profil aktiviert. Bei Aktivierung dieses Profils werden von Bitdefender Antivirus Plus 2018 automatisch die folgenden Programmeinstellungen vorgenommen:


- Die Erweiterte Gefahrenabwehr ist aktiviert
- 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.

17.3.4. 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.



18. 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.

18.1. 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.

18.2. 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.

18.3. 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.


18.4. 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.



19. 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 Anmeldeinformationen 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


19.1. 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**.

19.2. 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**.

19.3. 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.



19.4. 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.

19.5. 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**.



19.6. 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.

19.7. 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 Ausfüloptionen anzeigen** - Ein Pop-up-Fenster mit Ihren Ausfüloptionen 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.



20. 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.

20.1. 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.


20.2. 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**.

20.3. 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-Abonnements finden Sie im Kapitel *„Abonnements“* (S. 134).

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-Plattform weitergeleitet, wo Sie einen hilfreichen Artikel zur Nutzung der Bitdefender VPN lesen können.
- **Über** - Hier finden Sie Informationen zur installierten Version.

20.4. 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 Plus 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 Antivirus Plus 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.



21. 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 im Kapitel *„Passwortmanager-Schutz für Ihre Anmeldedaten“* (S. 124).

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.



21.1. 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.

21.2. 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 ausgewählt 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.

21.3. 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.



22. DATENSCHUTZ

22.1. 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, LÖSCHEN**, 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.



23. 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-Immunsierung 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 im Kapitel „*Automatische Schwachstellensuche*“ (S. 114).



SYSTEMOPTIMIERUNG



24. 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, das 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.
- 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 des Öffentlichen-WLAN-Profiles werden von Bitdefender Antivirus Plus 2018 automatisch die folgenden Programmeinstellungen vorgenommen:


- Die Erweiterte Gefahrenabwehr ist aktiviert
- Die folgenden Einstellungen des Internet-Schutzes werden aktiviert:
 - SSL scannen
 - Schutz gegen Betrug
 - Schutz vor Phishing-Attacken

24.1. 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.

24.2. 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.




24.3. 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 **Spieelliste** hinzufügen.

So fügen Sie Spiele manuell zur Spielliste 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 **Spielaliste**.
5. Klicken Sie auf **Hinzufügen**, um ein neues Spiel zur **Spielaliste** 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.

24.4. 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-Profiles

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**.

24.5. 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.



24.6. 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.



PROBLEMLÖSUNG



25. 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. 154)*
- *„Der Scan startet nicht“ (S. 156)*
- *„Ich kann eine App nicht mehr verwenden“ (S. 158)*
- *„Wie gehe ich vor, wenn Bitdefender eine sichere Website oder Online-Anwendung blockiert?“ (S. 159)*
- *„Wie gehe ich vor, wenn Bitdefender eine sichere Anwendung als Ransomware einstuft?“ (S. 160)*
- *„Wie man Bitdefender-Updates auch mit einer langsamen Internet-Verbindung durchführen kann“ (S. 161)*
- *„Bitdefender-Dienste antworten nicht“ (S. 161)*
- *„Das automatische Einfügen funktioniert bei meiner Geldbörse nicht“ (S. 162)*
- *„Entfernen von Bitdefender ist fehlgeschlagen“ (S. 163)*
- *„Mein System fährt nach der Installation von Bitdefender nicht mehr hoch“ (S. 164)*

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. 180)* beschrieben, kontaktieren.

25.1. 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 im Kapitel *„Wie entferne ich andere Sicherheitslösungen?“* (S. 77).

- **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 im Kapitel *„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.

25.2. 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 Antivirus Plus 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 Antivirus Plus 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 Antivirus Plus 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 im Kapitel *„Wie entferne ich andere Sicherheitslösungen?“* (S. 77).

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 Antivirus Plus 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 Antivirus Plus 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 Antivirus Plus 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. 180) beschrieben.

25.3. 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 eine 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 **B**-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. 180) beschrieben.

25.4. 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 **B**-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. 180) beschrieben.

25.5. 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 **B**-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.



25.6. 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.

25.7. 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 überprüfen 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 im Kapitel *„Wie entferne ich andere Sicherheitslösungen?“* (S. 77).

Sollte der Fehler weiterhin auftreten, wenden Sie sich bitte an unsere Support-Mitarbeiter, wie in Abschnitt *„Hilfe anfordern“* (S. 180) beschrieben.

25.8. 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. 180) beschrieben.

25.9. 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 Antivirus Plus 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 Antivirus Plus 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 Antivirus Plus 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.

25.10. 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. 79).

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 Antivirus Plus 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 Antivirus Plus 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 Antivirus Plus 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. 79).

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. 79).
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. 180) beschrieben.



26. 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. 168)*
- *„Wie gehe ich vor, wenn Bitdefender eine Bedrohung auf meinem Computer findet?“ (S. 173)*
- *„Wie entferne ich eine Bedrohung aus einem Archiv?“ (S. 174)*
- *„Wie entferne ich eine Bedrohung aus einem E-Mail-Archiv?“ (S. 175)*
- *„Wie gehe ich vor, wenn ich eine Datei für gefährlich halte?“ (S. 177)*
- *„Wobei handelt es sich bei den passwortgeschützten Dateien im Scan-Protokoll?“ (S. 177)*
- *„Wobei handelt es sich bei den übersprungenen Objekten im Scan-Protokoll?“ (S. 178)*
- *„Wobei handelt es sich bei den zu stark komprimierten Dateien im Scan-Protokoll?“ (S. 178)*
- *„Warum hat Bitdefender ein infizierte Datei automatisch gelöscht?“ (S. 178)*

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. 180) beschrieben, kontaktieren.

26.1. 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 Antivirus Plus 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 **B**-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. 169) 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. 170) 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. 171).
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**.



26.2. 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. 76).



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. 79).
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. 76).
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. 180) beschrieben.

26.3. 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. 180) beschrieben.



26.4. 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. 180) beschrieben.



26.5. 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. 180).

26.6. 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.



26.7. 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.

26.8. 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.

26.9. Warum hat Bitdefender eine 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.



KONTAKTIEREN SIE UNS



27. 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. 154) 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-Produkt heraus“* (S. 180)
- *„Kontaktieren Sie uns über unser Online-Support-Center“* (S. 181)

Kontaktieren Sie uns direkt aus Ihrem Bitdefender-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. Klicken 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.html> und kontaktieren Sie unseren Kundendienst.



28. 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.

28.1. 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 berechtigten 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>.



28.2. 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**.

28.3. 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>.



29. 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.

29.1. 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>

29.2. 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.

29.3. Bitdefender-Niederlassungen

Bitdefender-Niederlassungen stehen Ihnen für betriebliche und allgemeine Fragen und Informationen in ihren jeweiligen Bereichen jederzeit zur Verfügung.



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 EMail: 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 EMail: 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 Persistent 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 Programmiermodell, das 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 ActiveX die Sicherheitskontrollen fehlen, deshalb raten Computersicherheitsexperten davon ab, ActiveX 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. Andererseits 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 Netzwerkservers 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 Virens scanner 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 bössartiger 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 stattgefundenen 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 einer 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 Schnittstellenummer 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 böses 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.