

Bitdefender[®] **ANTIVIRUS FREE**



**BEDIENUNGSAN
LEITUNG**





Bitdefender Antivirus kostenlos

Bedienungsanleitung

Erscheinungsdatum 12.04.2023
Copyright © 2023 Bitdefender

Impressum

Alle Rechte vorbehalten. Kein Teil dieses Buches darf ohne schriftliche Genehmigung eines autorisierten Vertreters von Bitdefender in irgendeiner Form oder auf irgendeine Weise, elektronisch oder mechanisch, einschließlich Fotokopie, Aufzeichnung oder durch ein Informationsspeicher- und -abrufsystem, reproduziert oder übertragen werden. Die Aufnahme von Kurzzitaten in Rezensionen ist ggf. nur mit Quellenangabe möglich. Der Inhalt kann in keiner Weise verändert werden.

Warnung und Haftungsausschluss. Dieses Produkt und seine Dokumentation sind urheberrechtlich geschützt. Die Informationen in diesem Dokument werden „wie besehen“ ohne Gewährleistung bereitgestellt. Obwohl bei der Erstellung dieses Dokuments alle Vorsichtsmaßnahmen getroffen wurden, übernehmen die Autoren keine Haftung gegenüber natürlichen oder juristischen Personen in Bezug auf Verluste oder Schäden, die direkt oder indirekt durch die in diesem Werk enthaltenen Informationen verursacht wurden oder angeblich verursacht wurden.

Dieses Buch enthält Links zu Websites Dritter, die nicht unter der Kontrolle von Bitdefender stehen, daher ist Bitdefender nicht für den Inhalt verlinkter Websites verantwortlich. Wenn Sie auf eine in diesem Dokument aufgeführte Website eines Drittanbieters zugreifen, tun Sie dies auf eigene Gefahr. Bitdefender stellt diese Links nur als Annehmlichkeit zur Verfügung, und die Aufnahme des Links bedeutet nicht, dass Bitdefender den Inhalt der Website Dritter billigt oder irgendeine Verantwortung dafür übernimmt.

Warenzeichen. In diesem Buch können Markennamen vorkommen. Alle eingetragenen und nicht eingetragenen Warenzeichen in diesem Dokument sind das alleinige Eigentum ihrer jeweiligen Eigentümer und werden respektvoll anerkannt.

Bitdefender®



Inhaltsverzeichnis

Über diese Anleitung	1
Zielsetzung und Zielgruppe	1
So verwenden Sie dieses Handbuch	1
Konventionen in diesem Handbuch	1
Typografie	1
Zusätzliche Hinweise	2
Ihre Mithilfe	2
1. Installation	4
1.1. Vor der Installation	4
1.2. Systemanforderungen	4
1.3. Software-Anforderungen	5
1.4. Installieren Ihres Bitdefender-Produkts	6
1.4.1. Installation über Bitdefender Central	6
1.4.2. Installation vom Installationsdatenträger	9
2. Erste Schritte	15
2.1. Grundlagen	15
2.1.1. Benachrichtigungen	16
2.1.2. Profile	17
2.1.3. Passwortschutz für Bitdefender-Einstellungen	19
2.1.4. Produktberichte	20
2.1.5. Benachrichtigungen zu Sonderangeboten	20
2.2. Bitdefender-Benutzeroberfläche	21
2.2.1. Task-Leisten-Symbol	21
2.2.2. Navigationsmenü	23
2.2.3. Dashboard	24
2.2.4. Die Bereiche Ihres Bitdefender-Produkts	27
2.2.5. Produktsprache ändern	32
2.3. Bitdefender Central	32
2.3.1. Über Bitdefender Central	32
2.3.2. Aufrufen von Bitdefender Central	33
2.3.3. Zwei-Faktor-Authentifizierung	34
2.3.4. Hinzufügen vertrauenswürdiger Geräte	36
2.3.5. Aktivität	37
2.3.6. Meine Abonnements	37
2.3.7. Meine Geräte	39
2.3.8. Benachrichtigungen	43
2.4. Bitdefender auf dem neuesten Stand halten	43
2.4.1. Überprüfen, ob Bitdefender auf dem neuesten Stand ist ..	43
2.4.2. Durchführung eines Updates	44



2.4.3. Aktivieren / Deaktivieren der automatischen Updates	44
2.4.4. Update-Einstellungen anpassen	45
2.4.5. Regelmäßige Updates	46
3. Verwalten Ihrer Sicherheit	47
3.1. Virenschutz	47
3.1.1. Zugriff-Scans (Echtzeitschutz)	48
3.1.2. Bedarf-Scan	52
3.1.3. Scan-Protokolle lesen	62
3.1.4. Automatischer Scan von Wechselmedien	62
3.1.5. Konfigurieren der Scan-Ausnahmen	64
3.1.6. Verwalten von Dateien in Quarantäne	67
3.2. Erweiterte Bedrohungsabwehr	68
3.2.1. Aktivieren oder Deaktivieren der Advanced Threat Defense	68
3.2.2. Einsehen von erkannten schädlichen Angriffen	69
3.2.3. Hinzufügen von Prozessen zu den Ausnahmen	69
3.2.4. Exploits gefunden	70
3.2.5. Aktivieren oder Deaktivieren der Exploit-Erkennung	70
3.3. Abwehr von Online-Bedrohungen	70
3.3.1. Bitdefender-Benachrichtigungen im Browser	72
4. Gewusst wie	74
4.1. Installation	74
4.1.1. Wie kann ich Bitdefender auf einem zweiten Gerät installieren?	74
4.1.2. Wie kann ich Bitdefender erneut installieren?	74
4.1.3. Woher kann ich mein Bitdefender-Produkt herunterladen?	75
4.1.4. Wie kann ich ein Upgrade auf die neueste Bitdefender- Version durchführen?	76
4.2. Bitdefender-Zentrale	77
4.2.1. Wie kann ich mein Bitdefender-Benutzerkonto wechseln?	77
4.2.2. Wie kann ich die Bitdefender Central-Hilfemeldungen deaktivieren?	78
4.2.3. Ich habe das Passwort vergessen, das ich für mein Bitdefender-Konto festgelegt habe. Wie kann ich es zurücksetzen?	78
4.2.4. Wie kann ich die Benutzersitzungen in meinem Bitdefender-Konto verwalten?	79
4.3. Prüfen mit BitDefender	80
4.3.1. Wie kann ich eine Datei oder einen Ordner scannen?	80
4.3.2. Wie scanne ich mein System	80



4.3.3. Wie plane ich einen Scan?	80
4.3.4. Wie kann ich eine benutzerdefinierte Scan-Aufgabe anlegen?	81
4.3.5. Wie kann ich einen Ordner vom Scan ausnehmen?	83
4.3.6. Wie gehe ich vor, wenn Bitdefender eine saubere Datei als infiziert eingestuft hat?	84
4.3.7. Wo sehe ich, welche Bedrohungen Bitdefender gefunden hat?	85
4.4. Nützliche Informationen	86
4.4.1. Wie kann ich meine Sicherheitslösung selbst testen?	86
4.4.2. Wie kann ich Bitdefender deinstallieren?	87
4.4.3. Wie fahre ich das Gerät automatisch herunter, nachdem der Scan beendet wurde?	88
4.4.4. Wie konfiguriere ich Bitdefender für die Verwendung einer Proxy-Internetverbindung?	89
4.4.5. Ist auf meinem System die 32- oder 64-Bit-Version von Windows installiert?	90
4.4.6. Wie kann ich in Windows versteckte Objekte anzeigen?	91
4.4.7. Wie entferne ich andere Sicherheitslösungen?	92
4.4.8. Wie führe ich einen Neustart im abgesicherten Modus durch?	93
5. Problemlösung	96
5.1. Verbreitete Probleme beheben	96
5.1.1. Mein System scheint langsamer zu sein	96
5.1.2. Der Scan startet nicht	98
5.1.3. Ich kann eine App nicht mehr verwenden	100
5.1.4. Was können Sie tun, wenn Bitdefender eigentlich sichere Websites, Domains, IP-Adressen oder Online-Anwendungen blockiert?	101
5.1.5. Wie man Bitdefender-Updates auch mit einer langsamen Internet-Verbindung durchführen kann	102
5.1.6. Bitdefender-Dienste antworten nicht	103
5.1.7. Entfernen von Bitdefender fehlgeschlagen	104
5.1.8. Mein System fährt nach der Installation von Bitdefender nicht mehr hoch	105
5.2. Entfernung von Bedrohungen	108
5.2.1. Was ist zu tun, wenn Bitdefender Bedrohungen auf Ihrem Gerät findet?	109
5.2.2. Wie entferne ich eine Bedrohung aus einem Archiv?	110
5.2.3. Wie entferne ich eine Bedrohung aus einem E-Mail-Archiv?	112



5.2.4. Wie gehe ich vor, wenn ich eine Datei für gefährlich halte?	113
5.2.5. Wobei handelt es sich bei den passwortgeschützten Dateien im Scan-Protokoll?	113
5.2.6. Wobei handelt es sich bei den übersprungenen Objekten im Scan-Protokoll?	114
5.2.7. Wobei handelt es sich bei den zu stark komprimierten Dateien im Scan-Protokoll?	114
5.2.8. Warum hat Bitdefender eine infizierte Datei automatisch gelöscht?	114
6. Hilfe und Support	116
6.1. Hier wird Ihnen geholfen	116
6.2. Online-Ressourcen	116
6.2.1. Bitdefender-Support-Center	116
6.2.2. Die Bitdefender Experten Community	117
6.2.3. Bitdefender Cyberpedia	117
6.3. Kontaktinformation	118
6.3.1. Lokale Vertriebspartner	118
Glossar	119



ÜBER DIESE ANLEITUNG

Zielsetzung und Zielgruppe

Dieses Handbuch richtet sich an alle Windows-Benutzer, die sich für den Einsatz von Bitdefender Antivirus Free zum Schutz ihrer Computer entschieden haben. Die enthaltenen Informationen setzen keine besonderen Computerkenntnisse voraus, sondern dienen allen Windows-PC-Benutzern als leicht verständliche und hilfreiche Anleitung.

Es wird erklärt, wie Sie Bitdefender Antivirus Free konfigurieren und einsetzen, um sich vor Bedrohungen und Schadsoftware zu schützen, und wie sie Bitdefender optimal nutzen.

Viel Spaß mit diesen nützlichen und informativen Handbuch.

So verwenden Sie dieses Handbuch

Dieser Leitfaden ist um mehrere Hauptthemen herum organisiert:

[Erste Schritte \(Seite 15\)](#)

Beginnen Sie mit Bitdefender Free und seiner Benutzeroberfläche.

[Verwalten Ihrer Sicherheit \(Seite 47\)](#)

Erfahren Sie, wie Sie Bitdefender Free verwenden, um sich vor bösartiger Software zu schützen.

[Gewusst wie \(Seite 74\)](#)

Erfahren Sie mehr über Bitdefender Free.

[Hilfe und Support \(Seite 116\)](#)

Wo Sie suchen und um Hilfe bitten können, wenn etwas Unerwartetes auftaucht.

Konventionen in diesem Handbuch

Typografie

Zur Verbesserung der Lesbarkeit werden in diesem Handbuch verschiedene Textformate verwendet. Die Bedeutung der verschiedenen Formate können Sie der untenstehenden Tabelle entnehmen.



Erscheinungsbild	Beschreibung
Beispielsyntax	Syntaxbeispiele werden in einer Schriftart mit fester Laufweite angegeben.
https://www.bitdefender.de	Verweise (Links) auf externe Inhalte auf HTTP- oder FTP-Servern.
documentation@bitdefender.com	Verweise auf E-Mail-Adressen, z. B. zur Kontaktaufnahme.
Über diese Anleitung (Seite 1)	Interne Verweise (Links) auf beliebige Stellen innerhalb dieses Dokuments.
Dateiname	Dateien und Verzeichnisse werden in einer Schriftart mit fester Laufweite angegeben.
Option	Alle Produktoptionen werden fett gedruckt dargestellt.
Stichwort	Wichtige Stichwörter oder Begriffe werden durch Fettdruck hervorgehoben.

Zusätzliche Hinweise

Zusätzliche Hinweise sind im Text grafisch markiert und liefern ergänzende Informationen zum aktuellen Absatz, die Sie unbedingt beachten sollten.



Hinweis

Diese Bemerkung dient lediglich zur Überprüfung. Notizen enthalten nützliche Informationen wie zum Beispiel einen Verweis auf ein verwandtes Thema.



Wichtig

Diese Art von Hinweis sollte in jedem Fall gelesen werden. Es werden signifikante Informationen zum jeweiligen Thema bereitgestellt. Es wird nicht empfohlen diese zu übergehen.



Warnung

Diese kritische Information sollten Sie mit höchster Aufmerksamkeit verfolgen. Hier angegebenen Anweisungen und Informationen sollten Sie auf jeden Fall Beachtung schenken. Sie sollten diese Informationen sorgsam lesen und verstanden haben, da es sich um eine höchst prekäre Thematik handelt.

Ihre Mithilfe

Wir laden Sie dazu ein uns bei der Verbesserung dieses Dokuments mitzuhelfen. Wir haben sämtliche Informationen in diesem Dokument bestmöglich überprüft um somit die Qualität sicherzustellen.



Schicken Sie uns Ihre E-Mail an documentation@bitdefender.com. Bitte verfassen Sie bitte alle auf die Dokumentation bezogenen E-Mails auf Englisch.



1. INSTALLATION

1.1. Vor der Installation

Bevor Sie Bitdefender Antivirus Free installieren, sollten Sie für eine reibungslose Installation sicherstellen, dass folgende Schritte durchgeführt wurden:

- Stellen Sie sicher, dass das Zielgerät für die Bitdefender-Installation die Systemvoraussetzungen erfüllt. Wenn das Gerät die Systemvoraussetzungen nicht erfüllt, kann Bitdefender nicht installiert werden. Falls es doch installiert wird, kann es zu Leistungseinbußen und Stabilitätsproblemen kommen. Eine vollständige Liste der Systemanforderungen finden Sie im Kapitel [Systemanforderungen \(Seite 4\)](#).
- Melden Sie sich mit einem Administrator-Konto am Gerät an.
- Entfernen Sie alle anderen Sicherheitslösungen von Ihrem Gerät. Sollte während des Bitdefender-Installationsvorgangs welche gefunden werden, werden Sie aufgefordert, sie zu deinstallieren. Die gleichzeitige Nutzung mehrerer Sicherheitsprogramme kann die jeweilige Funktion stören und massive Probleme auf Ihrem Computer verursachen. Windows Defender wird während der Installation deaktiviert.
- Deaktivieren oder entfernen Sie jegliche Firewall-Programme, die auf dem Gerät installiert sind. Die gleichzeitige Nutzung mehrerer Sicherheitsprogrammen kann die jeweilige Funktion stören und massive Probleme auf Ihrem Computer verursachen. Die Windows-Firewall wird während der Installation deaktiviert.
- Ihr Gerät sollte während der Installation mit dem Internet verbunden sein, auch wenn Sie von CD oder DVD installieren. Falls neuere Versionen der Anwendungsdateien aus dem Installationspaket verfügbar sind, kann Bitdefender diese dann herunterladen und installieren.

1.2. Systemanforderungen

Sie können Bitdefender Antivirus Free nur auf Geräten mit den folgenden Betriebssystemen installieren:



- Windows 7 mit Service Pack 1
- Windows 8
- Windows 8.1
- Windows 10
- 2,5 GB verfügbarer Festplattenspeicher (davon mindestens 800 MB auf dem Systemlaufwerk)
- 2 GB Arbeitsspeicher (RAM)



Wichtig

Die Systemleistung kann auf Geräten mit CPUs der alten Generation beeinträchtigt werden.



Notiz

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

- Klicken Sie unter **Windows 7** auf Ihrem Desktop mit der rechten Maustaste auf **Arbeitsplatz** und wählen Sie im Menü **Eigenschaften** aus.
- Unter **Windows 8** finden Sie auf der Windows-Startseite den Eintrag **Computer** (z. B. durch Eingabe von "Computer" auf der Startseite). Rechtsklicken Sie auf das entsprechende Symbol. Suchen Sie unter **Windows 8.1** den Menüpunkt **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 Symbol. Im Abschnitt **System** finden Sie Informationen zu Ihrem Systemtyp.

1.3. Software-Anforderungen

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

- Ab Microsoft Edge 40
- Internet Explorer 10 und höher
- Mozilla Firefox 51 und höher
- Google Chrome 34 und höher



- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Ab Mozilla Thunderbird 14

1.4. Installieren Ihres Bitdefender-Produkts

Sie können Bitdefender vom Installationsdatenträger installieren oder den Web-Installer verwenden, der über **Bitdefender Central** auf Ihr Gerät heruntergeladen wird.

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

1.4.1. Installation über Bitdefender Central

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

So laden Sie Bitdefender Antivirus Free über Bitdefender Central herunter:

1. Rufen Sie **Bitdefender Central** auf.
2. Rufen Sie den Bereich **Meine Geräte** auf und klicken Sie auf **SCHUTZ INSTALLIEREN**.
3. Wählen Sie eine der beiden verfügbaren Optionen:
 - **Dieses Gerät schützen**
 - a. Wählen Sie diese Option und danach den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, klicken Sie auf die entsprechende Schaltfläche.
 - b. Speichern Sie die Installationsdatei.
 - **Andere Geräte schützen**
 - a. Wählen Sie diese Option und dann den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, klicken Sie auf die entsprechende Schaltfläche.
 - b. Klicken Sie auf **DOWNLOAD-LINK SENDEN**.



- c. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **E-MAIL VERSENDEN**.
Bitte beachten Sie, dass der generierte Download-Link nur für die nächsten 24 Stunden gültig ist. Nach Ablauf des Links müssen Sie einen neuen Link generieren. Führen Sie dazu die bereits beschriebenen Schritte erneut aus.
 - d. Rufen Sie auf dem Gerät, auf dem Bitdefender installiert werden soll, das angegebene E-Mail-Konto auf und klicken Sie in der E-Mail auf die Download-Schaltfläche.
4. Warten Sie, bis der Download abgeschlossen ist, und führen Sie das Installationsprogramm aus.

Validierung der Installation

Bitdefender überprüft zunächst Ihr System, um die Installation zu bestätigen.

Wenn Ihr System die Systemvoraussetzungen 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 Ihr Gerät neu starten, um die Entfernung der erkannten Sicherheitslösungen abzuschließen.

Das Installationspaket für Bitdefender Total Security wird regelmäßig aktualisiert.



Notiz

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

Sobald die Installation bestätigt ist, wird der Einrichtungsassistent angezeigt. Folgen Sie den Schritten zur Installation von Bitdefender Antivirus Free.

Schritt 1 - Bitdefender-Installation

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 Free 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 **Produktberichte 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.

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.

Schritt 4 - Geräteanalyse

Sie werden jetzt gefragt, ob Sie eine Analyse Ihres Geräts durchführen möchten, um sicherzustellen, dass es nicht gefährdet ist. In diesem Schritt wird Bitdefender kritische Systembereiche scannen. Klicken Sie zum Starten auf **Geräteanalyse starten**.

Sie können die Scan-Oberfläche ausblenden, indem Sie auf **Scan im Hintergrund ausführen** klicken. Legen Sie danach fest, ob Sie informiert werden möchten, wenn der Scan abgeschlossen ist.



Klicken Sie nach Abschluss des Scans auf **Bitdefender-Benutzeroberfläche öffnen**.



Notiz

Alternativ können Sie, wenn Sie den Scan nicht durchführen möchten, einfach auf **Überspringen** klicken.

Schritt 5 - Erste Schritte

Im Fenster **Erste Schritte** finden Sie weitere Einzelheiten zu Ihrem aktivem Abonnement.

Klicken Sie auf **ABSCHLIEßEN**, um die Benutzeroberfläche Bitdefender Antivirus Free aufzurufen.

1.4.2. 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 überprüft zunächst Ihr System, um die Installation zu bestätigen.

Wenn Ihr System die Systemvoraussetzungen 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 Ihr Gerät neu starten, um die Entfernung der erkannten Sicherheitslösungen abzuschließen.

Das Installationspaket für Bitdefender Total Security wird regelmäßig aktualisiert.



Notiz

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

Sobald die Installation bestätigt ist, wird der Einrichtungsassistent angezeigt. Folgen Sie den Schritten zur Installation von Bitdefender Antivirus Free.

Schritt 1 - Bitdefender-Installation

Bevor Sie mit der Installation fortfahren, müssen Sie dem Abonnementvertrag zustimmen. Bitte nehmen Sie sich etwas Zeit, um den Abonnementvertrag zu lesen, da er die Bedingungen enthält, unter denen Sie ihn verwenden dürfen Bitdefender Antivirus Free.

Wenn Sie diesen Bedingungen nicht zustimmen, schließen Sie das Fenster. Der Installationsvorgang wird abgebrochen und Sie beenden das Setup.

In diesem Schritt können zwei zusätzliche Aufgaben ausgeführt werden:

- ☐ Behalte das **Produktberichte versenden** Option aktiviert. Wenn Sie diese Option zulassen, werden Berichte mit Informationen darüber, wie Sie das Produkt verwenden, an die Bitdefender-Server gesendet. Diese Informationen sind für die Verbesserung des Produkts unerlässlich und können uns helfen, in Zukunft ein besseres Erlebnis zu bieten. Beachten Sie, dass diese Berichte keine vertraulichen Daten wie Ihren Namen oder Ihre IP-Adresse enthalten und nicht für kommerzielle Zwecke verwendet werden.
- ☐ Wählen Sie die Sprache aus, in der Sie das Produkt installieren möchten.

Klicken **INSTALLIEREN** um den Installationsprozess Ihres Bitdefender-Produkts zu starten.

Schritt 2 - Installation läuft

Warten Sie, bis die Installation abgeschlossen ist. Detaillierte Informationen zum Fortschritt werden angezeigt.



Schritt 3 - Installation abgeschlossen

Eine Zusammenfassung der Installation wird angezeigt. Wenn während der Installation eine aktive Bedrohung erkannt und entfernt wurde, ist möglicherweise ein Systemneustart erforderlich.

Schritt 4 – Geräteanalyse

Sie werden nun gefragt, ob Sie eine Analyse Ihres Geräts durchführen möchten, um sicherzustellen, dass es sicher ist. Während dieses Schritts scannt Bitdefender kritische Systembereiche. Klicken **Geräteanalyse starten** es zu initiieren.

Sie können die Scanoberfläche ausblenden, indem Sie auf klicken **Scan im Hintergrund ausführen**. Wählen Sie danach, ob Sie benachrichtigt werden möchten, wenn der Scan abgeschlossen ist, oder nicht.

Klicken Sie nach Abschluss des Scans auf **Weiter mit Konto erstellen**.



Notiz

Wenn Sie den Scan nicht durchführen möchten, können Sie alternativ einfach auf klicken **Überspringen**.

Schritt 5 - Bitdefender-Benutzerkonto

Nach Abschluss der ersten Einrichtung wird das Bitdefender Account-Fenster angezeigt. Zur Aktivierung des Produktes und zur Nutzung seiner Online-Funktionen wird ein Bitdefender-Benutzerkonto benötigt. Weitere Informationen finden Sie im Kapitel [Bitdefender-Zentrale](#).

Fahren Sie entsprechend Ihrer Situation fort.

☐ Ich möchte ein Bitdefender-Benutzerkonto anlegen

1. Geben Sie die Daten in die entsprechenden Felder ein. Die hier eingetragenen Daten bleiben vertraulich. Das Passwort muss mindestens 8 Zeichen enthalten, davon mindestens eine Ziffer, ein Sonderzeichen, einen Kleinbuchstaben und einen Großbuchstaben.
2. Bevor Sie fortfahren können, müssen Sie zunächst den Nutzungsbedingungen zustimmen. Rufen Sie die Nutzungsbedingungen auf und lesen Sie sie aufmerksam durch, da Sie hier die Bedingungen zur Nutzung von Bitdefender finden. Darüber hinaus können Sie auch die Datenschutzrichtlinie aufrufen und lesen.



3. Klicken Sie auf **BENUTZERKONTO ERSTELLEN**.



Notiz

Sobald das Benutzerkonto erstellt wurde, können Sie sich mit der angegebenen E-Mail-Adresse und dem Passwort unter <https://central.bitdefender.com> bei Ihrem Konto anmelden. Alternativ ist dies auch über die Bitdefender Central-App möglich, falls Sie diese auf einem Ihrer Android- oder iOS-Geräten installiert haben. Rufen Sie zur Installation der Bitdefender Central-App auf Ihrem Android-Gerät Google Play auf, suchen Sie Bitdefender Central und tippen Sie auf Installieren. Rufen Sie zur Installation der Bitdefender Central-App auf Ihrem iOS-Gerät den App Store auf, suchen Sie Bitdefender Central und tippen Sie auf Installieren.

○ Ich habe bereits ein Bitdefender-Benutzerkonto

1. Klicken Sie auf **Anmelden**.
2. Geben Sie die E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **WEITER**.
3. Geben Sie Ihr Passwort ein und klicken Sie auf **ANMELDEN**.
Wenn Sie das Passwort vergessen haben oder aus anderen Gründen zurücksetzen möchten, gehen Sie bitte wie folgt vor:
 - a. Klicken Sie auf **Passwort vergessen?**.
 - b. Geben Sie Ihre E-Mail-Adresse ein und klicken Sie auf **WEITER**.
 - c. Rufen Sie Ihre E-Mails ab, geben Sie den Sicherheitscode ein, den Sie per E-Mail bekommen haben, und klicken Sie auf **WEITER**.
Oder Sie klicken in der E-Mail, die Sie von uns bekommen haben, auf **Passwort ändern**.
 - d. Geben Sie das neue Passwort ein, das Sie festlegen möchten, und wiederholen Sie die Eingabe. Klicken Sie auf **SPEICHERN**.



Notiz

Wenn Sie bereits ein MyBitdefender-Konto haben, können Sie sich damit bei Ihrem Bitdefender-Konto anmelden. Wenn Sie Ihr Passwort vergessen haben, müssen Sie es zunächst unter <https://my.bitdefender.com> zurücksetzen. Verwenden Sie dann die aktualisierten Anmeldedaten, 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.

Notiz

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 6 - Produkt aktivieren

Notiz

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

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

Gehen Sie abhängig von Ihrer persönlichen Situation folgendermaßen vor:

Ich habe einen Aktivierungscode

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

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



Notiz

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 30 Tage lang nutzen. Um die Testphase zu beginnen, wählen Sie **Ich habe kein Abonnement, ich möchte das Produkt kostenlos testen**, und klicken Sie dann auf **FORTFAHREN**.

Schritt 7 - Erste Schritte

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

Klicken **BEENDEN** um auf die zuzugreifen Bitdefender Antivirus Free Schnittstelle.



2. ERSTE SCHRITTE

2.1. Grundlagen

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

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

Ungeschützte Verbindungen mit öffentlichen WLAN-Netzwerken in Flughäfen, Einkaufszentrum, Cafés oder Hotels geht 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-App](#) installieren.

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

[Webcam-Schutz](#) verhindert, dass nicht vertrauenswürdige Apps auf Ihre Kamera zugreifen und unterbindet so Hacking-Versuche. Der Bitdefender-Benutzer entscheidet, welche Apps auf Ihre Webcam zugreifen dürfen und welche blockiert werden.

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

Ab sofort können Sie durch Ransomware verschlüsselte Dateien wiederherstellen, ohne dafür das geforderte Lösegeld zahlen zu müssen.



Weitere Informationen zum Wiederherstellen von verschlüsselten Dateien finden Sie im Kapitel [Ransomware-Bereinigung](#).

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](#) ([Seite 17](#)).

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](#) ([Seite 16](#)).

Von Zeit zu Zeit sollten Sie Bitdefender öffnen und existierende Probleme beheben. Sie müssen zum Schutz Ihres Geräts und Ihrer Daten unter Umständen bestimmte Bitdefender-Komponenten konfigurieren oder vorbeugende Maßnahmen durchführen.

Rufen Sie Ihr Bitdefender-Benutzerkonto auf, um die Online-Funktionen von Bitdefender Antivirus Free zu nutzen und Ihre Abonnements und Geräte zu verwalten. Weitere Informationen finden Sie im Kapitel [Bitdefender-Zentrale](#).

Im Abschnitt [Gewusst wie](#) ([Seite 74](#)) finden Sie Schritt-für-Schritt-Anleitungen zur Durchführung der häufigsten Aufgaben. Wenn Sie Probleme beim Einsatz von Bitdefender haben, finden Sie im Abschnitt [Verbreitete Probleme beheben](#) ([Seite 96](#)) mögliche Lösungen für die häufigsten Probleme.

2.1.1. Benachrichtigungen

Bitdefender führt ein detailliertes Ereignisprotokoll über alle Aktivitäten der Software auf Ihrem Gerät. Für jedes Ereignis, das 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 auf dem Gerät gefunden wurden. Zudem können Sie bei



Bedarf weitere Aktionen ausführen oder die von Bitdefender ausgeführten Aktionen anpassen.

Klicken Sie im Navigationsmenü der **Bitdefender-Benutzeroberfläche** auf Benachrichtigungen, 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:

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

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

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

2.1.2. Profile

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

Bitdefender-Profile weisen den laufenden Apps mehr Systemressourcen zu, indem Sicherheitseinstellungen und einzelne Elemente der Systemkonfiguration vorübergehend angepasst werden. So wird der Ressourcenverbrauch insgesamt minimiert.

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



Arbeitsprofil

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

Filmprofil

Verbessert die visuellen Effekte und sorgt für störungsfreies Filmvergnügen.

Spielprofil

Verbessert die visuellen Effekte und sorgt für störungsfreies Spielvergnügen.

Öffentliches WLAN-Profil

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

Akkubetriebsprofil

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

Automatische Aktivierung von Profilen konfigurieren

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

Beim ersten Zugriff auf **Profile** werden Sie aufgefordert, automatische Profile zu aktivieren. Dazu können Sie im angezeigten Fenster einfach auf **AKTIVIEREN** klicken.

Sie können auf **JETZT NICHT** klicken, wenn Sie die Funktion zu einem späteren Zeitpunkt aktivieren möchten.

So erlauben Sie Bitdefender, Profile automatisch zu aktivieren:

1. Klicken Sie im Navigationsmenü der **Bitdefender-Benutzeroberfläche** auf **Dienstprogramme**.
2. Klicken Sie im Reiter **Profile** auf **Einstellungen**.
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 Schalter. Von den ersten drei Profilen kann nur eines gleichzeitig manuell aktiviert werden.

Weitere Informationen zu den Profilen finden Sie im Kapitel [Profile \(Seite 17\)](#).

2.1.3. Passwortschutz für Bitdefender-Einstellungen

Wenn Sie nicht die einzige Person mit Administratorrechten sind, die dieses Gerät verwendet, empfehlen wir Ihnen, Ihre Bitdefender-Einstellungen mit einem Passwort zu schützen.

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

1. Klicken Sie im Navigationsmenü der **Bitdefender-Benutzeroberfläche** auf **Einstellungen**.
2. Aktivieren Sie im Fenster **Allgemein** den **Passwortschutz**.
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 **Einstellungen** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Deaktivieren Sie im Fenster **Allgemein** den **Passwortschutz**.
3. Geben Sie das Passwort ein und klicken Sie auf **OK**.



Notiz

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

2.1.4. Produktberichte

Produktberichte enthalten Informationen darüber, wie Sie das bei Ihnen installierte Bitdefender-Produkt nutzen. 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.

Gehen Sie folgendermaßen vor, wenn Sie sich während der Installation für die Übermittlung von Produktberichten an die Bitdefender-Server entschieden haben und dies nun wieder rückgängig machen möchten:

1. Klicken **Einstellungen** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Wechseln Sie zum Reiter **Erweitert**.
3. Deaktivieren Sie **Produktberichte**.

2.1.5. 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 **Einstellungen** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Aktivieren oder deaktivieren Sie im Fenster **Allgemein** den entsprechenden Schalter.

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



2.2. Bitdefender-Benutzeroberfläche

Bitdefender Antivirus Free ist sowohl für Profis als auch für Computer-Neulinge geeignet. 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. Klicken Sie auf die Spitze Klammer rechts, um dem Assistenten weiter zu folgen, oder **Einführung überspringen**, um den Assistenten zu schließen.

Über das Bitdefender-**Taskleistensymbol** können Sie jederzeit das Hauptfenster öffnen, ein Produktupdate durchführen oder Informationen zur installierten Version abrufen.

Im Hauptfenster finden Sie Informationen zu Ihrem Sicherheitsstatus. Abhängig von Ihrer Gerätenutzung und Ihren Anforderungen, zeigt der **Autopilot** hier unterschiedliche Empfehlungen an, um Sie bei der Verbesserung Ihrer Gerätesicherheit und -leistung zu unterstützen. Sie können darüber hinaus Schnellaktionen für die von Ihnen am häufigsten genutzten Funktionen hinzufügen, damit Sie jederzeit darauf zugreifen können.

Über das Navigationsmenü links können Sie auf die Einstellungen, die Benachrichtigungen und die verschiedenen **Bitdefender-Bereiche** zugreifen, um das Produkt im Detail zu konfigurieren und auf erweiterte Administrationsaufgaben zuzugreifen.

Über den Bereich oben im Hauptfenster können Sie auf Ihr **Bitdefender-Benutzerkonto** zugreifen. Sie können auch jederzeit unseren Support kontaktieren, falls Sie noch Fragen haben oder unerwartete Probleme auftreten.

2.2.1. Task-Leisten-Symbol

Über das Bitdefender-Symbol  in der Taskleiste können Sie schneller auf das Produkt zugreifen.



Notiz

Das Bitdefender-Symbol wird möglicherweise nicht immer angezeigt. So können Sie das Symbol anheften:

○ Unter **Windows 7, Windows 8 und Windows 8.1**

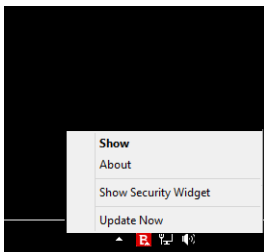
1. Klicken Sie auf den Pfeil  unten rechts im Bildschirm.
2. Klicken Sie auf **Benutzerdefiniert ...**, um das Fenster der Infobereichsymbole zu öffnen.
3. Legen Sie für das **Bitdefender Agent-Symbol** **Symbole und Benachrichtigungen anzeigen** fest.

○ Unter **Windows 10**

1. Klicken Sie mit der rechten Maustaste auf die Taskleiste und wählen Sie **Taskleisteneinstellungen**.
2. Scrollen Sie nach unten und klicken Sie unter **Infobereich** auf **Symbole für die Anzeige auf der Taskleiste auswählen**.
3. Aktivieren Sie den Schalter neben dem **Bitdefender Agent**.

Wenn Sie dieses Icon doppelklicken wird sich BitDefender öffnen. Zudem öffnen Sie durch einen Rechtsklick ein Untermenü welches Ihnen einen schnellen verwalten des BitDefender Produkts ermöglicht.

- **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 aufrufen und nachlesen können.
- **Jetzt Aktualisieren** - startet ein sofortiges Update. Sie können den Update-Status im Update-Bereich des **Bitdefender Hauptfensters** verfolgen.





Das Bitdefender-Taskleistensymbol zeigt an, ob Probleme Ihr Gerät oder die Funktionsweise des Produkts beeinträchtigen. Dabei werden die folgende Symbole angezeigt:

 Es gibt keine Probleme, die die Sicherheit Ihres Systems beeinträchtigen.

 Kritische Probleme beeinträchtigen die Sicherheit Ihres Systems. Sie benötigen Ihre sofortige Aufmerksamkeit und müssen umgehend behoben werden.

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

2.2.2. Navigationsmenü

Links in der Bitdefender-Benutzeroberfläche finden Sie das Navigationsmenü, über das Sie schnell und bequem auf die Bitdefender-Funktionen und -Tools zur Nutzung Ihres Produkts zugreifen können. In diesem Bereich finden Sie die folgenden Reiter:

-  **Dashboard.** Von hier aus können Sie Sicherheitsprobleme schnell beheben, Empfehlungen anzeigen, die sich aus Ihren Systemanforderungen und Ihrem Nutzungsverhalten ableiten, Schnellaktionen durchführen und Bitdefender auf weiteren Geräten installieren.
-  **Schuz.** Von hier aus können Sie Virenschutz-Scans starten und konfigurieren, auf die Firewall-Einstellungen zugreifen, eventuell durch Ransomware verschlüsselte Daten wiederherstellen und den Schutz beim Surfen im Internet konfigurieren.
-  **Privatsphäre.** Von hier aus können Sie Passwortmanager für Ihre Online-Benutzerkonten erstellen, Ihre Webcam vor Zugriff durch Unbefugte schützen, Online-Zahlungen in einer sicheren Umgebung vornehmen, die VPN-App öffnen und Ihre Kinder schützen, indem Sie ihre Online-Aktivitäten einsehen und einschränken.



-  **Dienstprogramme.** Von hier aus können Sie Ihre Systemgeschwindigkeit verbessern und die Diebstahlsicherung für Ihre Geräte konfigurieren.
-  **Benachrichtigungen.** Von hier aus können Sie auf Ihre Benachrichtigungen zugreifen.
-  **Einstellungen.** Von hier aus können Sie auf die allgemeinen Einstellungen zugreifen.
-  **Support.** Von hier aus können Sie sich direkt an den technischen Support von Bitdefender wenden, wenn Sie Hilfe bei der Lösung eines Problems mit Bitdefender Antivirus Free benötigen.
-  **Mein Konto.** Von hier aus können Sie Ihr Bitdefender-Benutzerkonto aufrufen, um Ihre Abonnements einzusehen und auf den von Ihnen verwalteten Geräten Sicherheitsaufgaben ausführen. Hier finden Sie auch Einzelheiten zu Ihrem Bitdefender-Benutzerkonto und dem aktuell verwendeten Abonnement.

2.2.3. Dashboard

Im [Dashboard-Fenster 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 drei Hauptbereiche aufgeteilt:

Sicherheitsstatusbereich

Hier können Sie den Sicherheitsstatus Ihres Geräts überprüfen.

Autopilot

Hier können Sie die Empfehlungen des Autopilots einsehen, um eine einwandfreie Funktion des Systems zu gewährleisten.

Schnellaktion

Hier können Sie verschiedene Aufgaben ausführen, um Ihr System zu schützen und Systemressourcen optimal zu nutzen. Sie können Bitdefender zudem auf anderen Geräten installieren, sofern Ihr Abonnement genügend freie Arbeitsplätze hat.



Sicherheitsstatusbereich

Bitdefender nutzt ein System zur Problemverfolgung, um potenzielle Sicherheitsprobleme für Ihr Gerät 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.

Wenn Probleme die Sicherheit Ihres Geräts beeinträchtigen, wechselt die Farbe der Statusanzeige oben rechts in der **Bitdefender-Benutzeroberfläche** auf rot. Der angezeigte Status informiert Sie über die Art der Probleme, die Ihr System beeinträchtigen. Darüber hinaus wechselt das Symbol in der **Taskleiste** zu . Wenn Sie den Mauszeiger über das Symbol bewegen, bestätigt ein Pop-up-Fenster das Vorliegen ausstehender Probleme.

Da die erkannten Probleme verhindern könnten, dass Bitdefender Sie vor Bedrohungen schützt, bzw. auf ein ernstes Sicherheitsrisiko hinweisen könnten, empfehlen wir ein sofortiges Eingreifen und eine umgehende Behebung der Probleme. Klicken Sie auf die Schaltfläche neben dem erkannten Problem, um es zu beheben.

Autopilot

Um einen wirksamen Betrieb und noch besseren Schutz bei Ihren verschiedenen Aktivitäten sicherzustellen, fungiert der Bitdefender Autopilot als Ihr persönlicher Sicherheitsberater. Je nachdem, was Sie gerade machen - egal, ob Sie arbeiten, Online-Zahlungen durchführen, Filme schauen oder spielen - der Bitdefender Autopilot liefert Ihnen kontextabhängige Empfehlungen, die sich an Ihrer Gerätenutzung und an Ihren Anforderungen orientieren.

Die vorgeschlagenen Empfehlungen können auch Maßnahmen umfassen, die Sie ergreifen sollten, um einen optimalen Betrieb Ihres Produkts sicherzustellen.

Klicken Sie auf die entsprechende Schaltfläche, um eine empfohlene Funktion zu nutzen oder Verbesserungen an Ihrem Produkt vorzunehmen.

Deaktivieren der Autopilot-Benachrichtigungen

Um Sie auf die Empfehlungen des Autopilots aufmerksam zu machen, zeigt Ihr Bitdefender-Produkt standardmäßig entsprechende Pop-up-Benachrichtigungen an.



So können Sie die Autopilot-Benachrichtigungen deaktivieren:

1. Klicken **Einstellungen** im Navigationsmenü auf der **Bitdefender-Oberfläche**.
2. Deaktivieren Sie im Fenster **Allgemein** die Option **Benachrichtigungen zu Empfehlungen**.

Schnellaktionen

Über die Schnellaktionen können Sie schnell und bequem Aufgaben starten, die Sie für den Schutz und die optimale Geschwindigkeit Ihres System als wichtig erachten.

Bitdefender umfasst standardmäßig eine Reihe von Schnellaktionen, die Sie jederzeit durch die von Ihnen am meisten genutzten Aktionen ersetzen können. So können Sie eine Schnellaktion ersetzen:

1. Klicken Sie auf das -Symbol oben rechts in der Karte, die Sie entfernen möchten.
2. Bewegen Sie den Mauszeiger auf die Karte, die Sie zum Hauptfenster hinzufügen möchten, und klicken Sie danach auf **HINZUFÜGEN**.

Sie können die folgenden Aufgaben zum Hauptfenster hinzufügen:

- **Quick Scan.** Führen Sie einen Quick Scan durch, um umgehend potenzielle Bedrohungen zu identifizieren, die auf Ihrem Gerät vorliegen könnten.
- **System-Scan.** Führen Sie einen System-Scan durch, um sicherzustellen, dass Ihr Gerät frei von Bedrohungen ist.
- **Schwachstellen-Scan.** Suchen Sie auf Ihrem Gerät nach Schwachstellen, um sicherzustellen, dass alle installierten Anwendungen und Ihr Betriebssystem auf dem neuesten Stand sind und ordnungsgemäß laufen.
- **WLAN-Sicherheitsberater.** Öffnen Sie das Fenster WLAN-Sicherheitsberater im Modul Schwachstellen.
- **Geldbörsen.** Zeigen Sie Ihre Geldbörsen an und verwalten Sie sie.
- **Safepay öffnen.** Öffnen Sie Bitdefender Safepay™, um Ihre sensiblen Daten bei Online-Transaktionen zu schützen.
- **VPN öffnen.** Öffnen Sie das Bitdefender VPN, um eine zusätzliche Schutzebene zwischen Ihren Geräten und dem Internet zu schaffen.



- **Dateischredder.** Starten Sie den Dateischredder, um sensible Daten spurlos von Ihrem Gerät zu löschen.
- **Ein-Klick-Optimierung öffnen.** Gewinnen Sie Speicherplatz auf der Festplatte, beheben Sie Registry-Fehler und schützen Sie Ihre Privatsphäre, indem Sie nicht mehr benötigte Dateien mit nur einem Klick löschen.

So können Sie weitere Geräte mit Bitdefender schützen:

1. Klicken Sie auf **Auf weiterem Gerät installieren**.
Ein neues Fenster wird angezeigt.
2. Klicken Sie auf **DOWNLOAD-LINK SENDEN**.
3. Folgen Sie den angezeigten Schritten, um Bitdefender zu installieren.

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

- Bitdefender Antivirus Free auf Windows-Geräten.
- Bitdefender Antivirus for Mac auf macOS-Geräten.
- Bitdefender Mobile Security auf Android-Geräten.
- Bitdefender Mobile Security auf iOS-Geräten.

2.2.4. Die Bereiche Ihres Bitdefender-Produkts

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

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

-  **Schutz**
-  **Privatsphäre**
-  **Dienstprogramme**

Schutz

Im Bereich Schutz können Sie erweiterte Sicherheitseinstellungen vornehmen, Freunde und Spammer verwalten, die Netzwerkverbindungseinstellungen anzeigen und bearbeiten, die



Funktionen des Online-Bedrohungsschutzes konfigurieren, nach möglichen Sicherheitslücken im System suchen und diese beheben sowie die Sicherheit genutzter Drahtlosnetzwerke prüfen.

Im Bereich Schutz können Sie die folgenden Funktionen verwalten:

VIRENSCHUTZ

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
- ☐ Rettungsumgebung

Weitere Informationen zu den Scan-Aufgaben und eine Anleitung, wie Sie den Virenschutz konfigurieren können, finden Sie im Kapitel [Virenschutz \(Seite 47\)](#).

ONLINE-GEFAHRENABWEHR

Mit der Online-Gefahrenabwehr schützen Sie sich beim Surfen im Netz zuverlässig vor Phishing-Angriffen, Betrugsversuchen und der Offenlegung privater Daten.

Weitere Informationen, wie man Bitdefender zum Schutz Ihrer Internet-Aktivitäten konfigurieren kann, finden Sie im Kapitel [Abwehr von Online-Bedrohungen \(Seite 70\)](#).

FIREWALL

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

Weitere Informationen zur Firewall-Konfiguration finden Sie im Kapitel [Firewall](#).

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 Bedrohungsabwehr \(Seite 68\)](#).

SPAM-SCHUTZ

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

Weitere Informationen zum Spam-Schutz finden Sie im Kapitel [Spam-Schutz](#).

SCHWACHSTELLE

Im Modul Schwachstelle können Sie Ihr Betriebssystem und Ihre am häufigsten verwendeten Anwendungen auf dem neuesten Stand halten und ungesicherte Drahtlosnetzwerke aufspüren. Klicken Sie auf **Öffnen** im Modul Schwachstellen, um auf die entsprechenden Funktionen zuzugreifen.

Mit dem **Schwachstellen-Scan** finden Sie kritische Windows-Updates, Anwendungsupdates, schwache Passwörter für Windows-Konten und unsichere WLAN-Netzwerke. Klicken Sie auf **Scan starten**, um einen Scan auf Ihrem Gerät durchzuführen.

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](#).

RANSOMWARE-BEREINIGUNG

Mit der Funktion für die Ransomware-Bereinigung können Sie Dateien auch dann wiederherstellen, wenn Sie durch Ransomware verschlüsselt wurden.

Weitere Informationen zum Wiederherstellen von verschlüsselten Dateien finden Sie im Kapitel [Ransomware-Bereinigung](#).

Privatsphäre

Im Bereich Privatsphäre können Sie die Bitdefender VPN-App öffnen, Ihre persönlichen Daten verschlüsseln, Ihre Online-Transaktionen schützen, Ihre



Webcam und Ihr Surf-Erlebnis absichern und Ihre Kinder schützen, indem Sie Ihre Online-Aktivitäten einsehen und einschränken.

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](#).

VIDEO- & AUDIO-SCHUTZ

Der Video- & Audioschutz sichert Ihre Webcam, indem es den Zugriff durch nicht vertrauenswürdige Anwendungen blockiert und Sie benachrichtigt, wenn Anwendungen versuchen, auf Ihr Mikrofon zuzugreifen.

Weitere Informationen darüber, wie Sie Ihre Webcam vor unerwünschtem Zugriff schützen können und wie Sie Bitdefender so konfigurieren, dass Sie über die Aktivitäten Ihres Mikrofons informiert werden, finden Sie unter [Video- & Audioschutz](#).

PASSWORD MANAGER

Der Bitdefender Password Manager 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](#).

SAFEPAY

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

Weitere Informationen zu Bitdefender Safepay™ finden Sie unter [Sichere Online-Transaktionen mit Safepay](#).

KINDERSICHERUNG

Mit der Bitdefender-Kindersicherung behalten Sie die Aktivitäten Ihrer Kinder auf ihren Geräten immer im Auge. Zum Schutz vor unangemessenen Inhalten können Sie entscheiden, ob ihr Zugang zum Internet oder zu bestimmten Apps eingeschränkt werden soll.



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

Weitere Informationen zur Konfiguration der Kindersicherung finden Sie in Kapitel [Kindersicherung](#).

ANTI-TRACKER

Die Anti-Tracker-Funktion hilft Ihnen, Tracking zu vermeiden, so dass Ihre Daten während des Surfs im Netz privat bleiben. Außerdem laden die von Ihnen aufgerufenen Websites schneller.

Weitere Informationen zur Anti-Tracker-Funktion finden Sie unter [Anti-Tracker](#).

Dienstprogramme

Im Bereich Dienstprogramme können Sie Ihre Systemgeschwindigkeit steigern und Ihre Geräte verwalten.

Ein-Klick-Optimierung

Bitdefender Total Security verschafft Ihnen nicht nur Sicherheit, sondern hilft Ihnen auch, die Leistung Ihres Geräts sicherzustellen.

Mit unserer Ein-Klick-Optimierung können Sie nicht mehr benötigte Dateien in einem einfachen Schritt finden und von Ihrem Gerät entfernen.

Weitere Informationen finden Sie im Kapitel [OneClick-Optimierer](#).

Diebstahlschutz

Der Bitdefender-Diebstahlschutz schützt Ihr Gerät und Ihre Daten bei Diebstahl oder Verlust. Im Falle der Fälle können Sie Ihr Gerät aus der Ferne orten oder sperren. Sie können zudem alle auf Ihrem Gerät gespeicherten Daten löschen.

Der Bitdefender-Diebstahlschutz umfasst die folgenden Funktionen:

- ☐ Fernortung
- ☐ Fernsperrung
- ☐ Fernlöschung
- ☐ Fernbenachrichtigung

Weitere Informationen zum Schutz Ihres Systems vor unbefugtem Zugriff finden Sie im Kapitel [Diebstahlschutz für Geräte](#).

Datenschutz



Der Bitdefender-Dateischredder hilft Ihnen, Daten endgültig zu löschen, indem er sie physisch von der Festplatte entfernt.

Weitere Informationen dazu finden Sie unter [Datenschutz](#).

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.

Weitere Informationen zu dieser Funktion finden Sie unter [Profile](#).

2.2.5. Produktsprache ändern

Die Bitdefender-Benutzeroberfläche ist in mehreren Sprachen verfügbar. Gehen Sie zum Ändern der Sprache wie folgt vor:

1. Klicken **Einstellungen** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Klicken Sie im Fenster **Allgemein** auf **Sprache ändern**.
3. Wählen Sie die gewünschte Sprache aus der Liste aus und klicken Sie auf **SPEICHERN**.
4. Warten Sie einen Moment, bis die Einstellungen übernommen wurden.

2.3. Bitdefender Central

2.3.1. Über Bitdefender Central

Bitdefender Central ist die Plattform, über die Sie Zugriff auf sämtliche Online-Funktionen und -Dienste des Produkts haben und über die Sie wichtige Aktionen auch per Fernzugriff auf Geräten ausführen können, auf denen Bitdefender installiert ist. Unter <https://central.bitdefender.com> können Sie sich von jedem mit dem Internet verbundenen Computer oder Mobilgerät aus bei Ihrem Bitdefender-Konto anmelden. Auf Android- und iOS-Geräten können Sie Bitdefender Central auch über die dazugehörige App aufrufen.

So können Sie die Bitdefender-Central-App auf Ihren Geräten installieren:



- **Android** - Suchen Sie Bitdefender Central in Google Play, laden Sie die App herunter und installieren Sie sie. Folgen Sie den Anweisungen, um die Installation abzuschließen.
- **iOS** - Suchen Sie Bitdefender Central im App Store, laden Sie die App herunter und installieren Sie sie. Folgen Sie den Anweisungen, um die Installation abzuschließen.

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:
 - Die Bitdefender-Produktlinie für Windows
 - Bitdefender Antivirus for Mac
 - Bitdefender Mobile Security for 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.
- Mit dem **Diebstahlschutz** schützen Sie Ihre Netzwerkgeräte und die darauf gespeicherten Daten vor Verlust und Diebstahl.
- Konfigurieren Sie die Einstellungen der **Kindersicherung** für die Geräte Ihrer Kinder und überwachen Sie ihre Aktivitäten jederzeit und überall.

2.3.2. Aufrufen von Bitdefender Central

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

- Ausgehend vom Bitdefender-Hauptfenster:
 1. Klicken Sie im Navigationsmenü der **Bitdefender-Benutzeroberfläche** auf **Mein Konto**.
 2. Klicken Sie auf **Bitdefender Central aufrufen**.



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 Konto an.
 - Über Ihr Android- oder iOS-Gerät:
 1. Öffnen Sie die von Ihnen installierte Bitdefender Central-App.



Notiz

Hier finden Sie alle Optionen, die Ihnen über die Web-Oberfläche zur Verfügung gestellt werden.

2.3.3. Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung fügt Ihrem Bitdefender-Benutzerkonto eine weitere Sicherheitsebene hinzu, indem sie zusätzlich zu Ihren Anmeldeinformationen einen Authentifizierungscode anfordert. Auf diese Weise verhindern Sie unbefugten Zugriff auf Ihr Benutzerkonto und schützen sich vor Cyberangriffen wie Keylogger-, Brute-Force- oder Wörterbuchangriffen.

Aktivieren der Zwei-Faktor-Authentifizierung

Durch die Aktivierung der Zwei-Faktor-Authentifizierung wird Ihr Bitdefender-Benutzerkonto deutlich besser abgesichert. Sie müssen Ihre Identität für jede Anmeldung über ein neues Gerät erneut bestätigen, so zum Beispiel wenn Sie eines der Bitdefender-Produkte installieren, Ihren Abonnementstatus einsehen oder per Fernzugriff Aufgaben auf Ihren Geräten ausführen.

So aktivieren Sie die Zwei-Faktor-Authentifizierung:

1. Zugang [Bitdefender-Zentrale](#).
2. Klicken Sie oben rechts auf dem Bildschirm auf das Symbol .



3. Klicken Sie im Schiebemenü auf **Bitdefender-Konto**.
4. Wechseln Sie zum Reiter **Passwort und Sicherheit**.
5. Klicken Sie auf **Zwei-Faktor-Authentifizierung**.
6. Tippen Sie auf **ERSTE SCHRITTE**.
Wählen Sie eine der folgenden Methoden aus:

- **Authentifizierungsanwendung** - Verwenden Sie eine Authentifizierungsanwendung, um für jede Anmeldung bei Ihrem Bitdefender-Konto einen Code zu generieren.

Wenn Sie eine Authentifizierungs-App verwenden möchten, sich aber nicht sicher sind, welche App Sie verwenden sollen, können Sie sie aus einer Liste mit den von uns empfohlenen Authentifizierungs-Apps auswählen.

- a. Klicken Sie zunächst auf **AUTHENTIFIZIERUNGSANWENDUNG VERWENDEN**.
- b. Verwenden Sie zur Anmeldung auf einem Android- oder iOS-Gerät Ihr Gerät, um den QR-Code zu scannen.
Zur Anmeldung auf einem Laptop oder Computer können Sie den angezeigten Code manuell eingeben.
Tippen Sie auf **FORTFAHREN**.
- c. Geben Sie den von der App generierten bzw. den im vorherigen Schritt angezeigten Code ein, und klicken Sie dann auf **AKTIVIEREN**.

- **E-Mail** - Bei jeder Anmeldung an Ihrem Bitdefender-Konto wird ein Bestätigungscode an Ihre E-Mail-Adresse gesendet. Rufen Sie Ihre E-Mails ab und verwenden Sie den erhaltenen Code.

- a. Klicken Sie zunächst auf **E-MAIL VERWENDEN**.
- b. Rufen Sie Ihre E-Mails ab, und geben Sie den erhaltenen Code ein.
- c. Tippen Sie auf **AKTIVIEREN**.
- d. Sie erhalten zehn Aktivierungscodes. Sie können die Liste entweder kopieren, herunterladen oder ausdrucken und für den Fall verwenden, dass Sie Ihre E-Mail-Adresse verlieren oder sich nicht mehr anmelden können. Jeder Code kann nur einmal verwendet werden.



- e. Klicken Sie auf **FERTIG**.

Gehen Sie folgendermaßen vor, wenn Sie die Zwei-Faktor-Authentifizierung nicht mehr nutzen möchten:

1. Klicken Sie auf **ZWEI-FAKTOR-AUTHENTIFIZIERUNG DEAKTIVIEREN**.
2. Sehen Sie in die App oder rufen Sie Ihre E-Mails ab, und geben Sie den erhaltenen Code ein.
Falls Sie sich für den Empfang des Authentifizierungs_codes per E-Mail entschieden haben, haben Sie fünf Minuten Zeit, um Ihre E-Mails abzurufen und den generierten Code einzugeben. Nach Ablauf dieser Zeit müssen Sie einen neuen Code generieren, indem Sie die gleichen Schritte erneut ausführen.
3. Bestätigen Sie Ihre Auswahl.

2.3.4. Hinzufügen vertrauenswürdiger Geräte

Um sicherzustellen, dass nur Sie auf Ihr Bitdefender-Konto zugreifen können, fragen wir unter Umständen zunächst einen Sicherheitscode ab. Wenn Sie bei Anmeldungen über das gleiche Gerät diesen Schritt überspringen möchten, empfehlen wir, dass Sie ein vertrauenswürdiges Gerät festzulegen.

So können Sie Geräte als vertrauenswürdige Geräte festlegen:

1. Zugang [Bitdefender-Zentrale](#).
2. Drücke den  Symbol oben rechts auf dem Bildschirm.
3. Klicken **Bitdefender-Konto** im Folienmenü.
4. Wähle aus **Passwort und Sicherheit** Tab.
5. Tippen Sie auf **Vertrauenswürdige Geräte**.
6. Es wird eine Liste mit Geräten angezeigt, auf denen Bitdefender installiert ist. Klicken Sie auf das gewünschte Gerät.

Sie können beliebig viele Geräte hinzufügen, vorausgesetzt, dass Bitdefender auf ihnen installiert ist und Sie über ein gültiges Abonnement verfügen.



2.3.5. Aktivität

Im Bereich Aktivität können Sie Informationen zu den Geräten einsehen, auf denen Bitdefender installiert ist.

Im Fenster **Aktivität** können Sie auf die folgenden Kacheln zugreifen:

- **Meine Geräte.** Hier können Sie die Anzahl der verbundenen Geräte sowie ihren jeweiligen Schutzstatus anzeigen. Um per Fernzugriff Probleme auf den erkannten Geräten zu beheben, klicken Sie auf **Probleme beheben** und dann auf **SCANNEN UND PROBLEME BEHEBEN**.

Um Details zu den erkannten Problemen anzuzeigen, klicken Sie auf **Probleme anzeigen**.

Von iOS-Geräten können keine Informationen zu erkannten Bedrohungen abgerufen werden.

- **Bedrohungen blockiert.** Hier können Sie ein Diagramm mit einer Gesamtstatistik mit Informationen über die blockierten Bedrohungen der letzten 24 Stunden bzw. 7 Tage anzeigen. Die angezeigten Informationen werden abhängig von dem schädlichen Verhalten abgerufen, das bei den aufgerufenen Dateien, Anwendungen und URLs erkannt wurde.
- **Benutzer mit den meisten blockierten Bedrohungen.** Hier können Sie eine Übersicht mit den Anwendern anzeigen, bei denen die meisten Bedrohungen gefunden wurden.
- **Geräte mit den meisten blockierten Bedrohungen.** Hier können Sie eine Übersicht mit den Geräten anzeigen, auf denen die meisten Bedrohungen gefunden wurden.

2.3.6. Meine Abonnements

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

Verfügbare Abonnements anzeigen

So können Sie Ihre verfügbaren Abonnements anzeigen:

1. Zugang [Bitdefender Central](#).
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.



Hinweis

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.

Abonnement aktivieren

Sie können ein Abonnement während des Installationsvorgangs mithilfe Ihres Bitdefender-Kontos aktivieren. Sobald die Aktivierung abgeschlossen ist, beginnt die Laufzeit des Abonnements.

Falls Sie einen Aktivierungscode von einem unserer Wiederverkäufer gekauft oder diesen als Geschenk erhalten haben, können Sie die Gültigkeitsdauer Ihres Bitdefender-Abonnements um diesen Zeitraum verlängern.

So können Sie Ihr Abonnement mit einem Aktivierungscode aktivieren:

1. Zugang [Bitdefender Central](#).
2. Wähle aus **Meine Abonnements** Tafel.
3. Klicken Sie auf **AKTIVIERUNGSCODE** und geben Sie den Code in das entsprechende Feld ein.
4. 2Klicken Sie zum Fortfahren auf **AKTIVIEREN**.

Das Abonnement wurde aktiviert.

Abonnement verlängern

Falls Sie die automatische Verlängerung Ihres Bitdefender-Abonnements deaktiviert haben, können Sie es auch selbst verlängern. Gehen Sie dazu wie folgt vor:

1. Zugang [Bitdefender Central](#).
2. Wähle aus **Meine Abonnements** Tafel.
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.

2.3.7. Meine Geräte

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

Hinzufügen eines neuen Geräts

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

1. Zugang [Bitdefender Central](#).
2. Wähle aus **Meine Geräte** Bedienfeld und tippen Sie dann auf **SCHUTZ INSTALLIEREN**.
3. Wählen Sie eine der beiden verfügbaren Optionen:

☐ **Schützen Sie dieses Gerät**

Wählen Sie diese Option und dann den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, tippen Sie auf die entsprechende Schaltfläche.

☐ **Schützen Sie andere Geräte**

Wählen Sie diese Option und dann den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, tippen Sie auf die entsprechende Schaltfläche.

Klicken Sie auf **DOWNLOAD LINK SENDEN**. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **E-MAIL VERSENDEN**. Bitte beachten Sie, dass der generierte Download-Link nur für die nächsten 24 Stunden gültig ist. Nach Ablauf des Links müssen Sie einen neuen Link generieren. Führen Sie dazu die bereits beschriebenen Schritte erneut aus.

Überprüfen Sie auf dem Gerät, auf dem Sie Ihr Bitdefender-Produkt installieren möchten, das E-Mail-Konto, das Sie eingegeben haben, und tippen Sie dann auf die entsprechende Download-Schaltfläche.



4. Warten Sie, bis der Download abgeschlossen ist, und führen Sie das Installationsprogramm aus.

Persönliche Anpassungen

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

1. Zugang [Bitdefender Central](#).
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 **Einstellungen**.
5. Geben Sie einen neuen Namen in das Feld **Geräte** ein und klicken Sie dann auf **SPEICHERN**.

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

1. Zugang [Bitdefender Central](#).
2. Wähle aus **Meine Geräte** Tafel.
3. Tippen Sie auf die gewünschte Gerätekarte und dann auf  Symbol in der oberen rechten Ecke des Bildschirms.
4. Wählen Sie **Profil**.
5. Klicken Sie auf **Besitzer hinzufügen** und füllen Sie im Anschluss die entsprechenden Felder aus. Passen Sie das Profil nach Bedarf an, indem Sie ein Foto hinzufügen, einen Geburtstag auswählen und eine E-Mail-Adresse sowie eine Telefonnummer eingeben.
6. Klicken Sie auf **HINZUFÜGEN**, um das Profil zu speichern.
7. Wählen Sie aus der Liste der **Gerätebesitzer** den gewünschten Besitzer aus und klicken Sie auf **ZUORDNEN**.

Fernzugriffsaktionen

So können Sie Bitdefender per Fernzugriff auf Ihren Geräten aktualisieren:

1. Zugang [Bitdefender Central](#).
2. Wähle aus **Meine Geräte** Tafel.



3. Tippen Sie auf die gewünschte Gerätekarte und dann auf  Symbol in der oberen rechten Ecke des Bildschirms.

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 werden Details zum ausgewählten Gerät angezeigt sowie sein Sicherheitsstatus, der Status des Bitdefender VPN und wie viele Bedrohungen in den vergangenen 7 Tagen blockiert wurden. 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. Wenn Probleme bestehen, klicken Sie auf das Klappmenü oben im Statusbereich, um mehr Details dazu anzuzeigen. Hier können Sie
- **Schutz.** Von diesem Fenster aus können Sie Quick- und System-Scans auf Ihrem Gerät durchführen. Klicken Sie dazu auf die Schaltfläche **SCANNEN**. Hier können Sie auch einsehen, wann der letzte Scan auf dem Gerät durchgeführt wurde, und einen Bericht mit den wichtigsten Informationen zum letzten Scan aufrufen.
- **Optimierung.** Hier können Sie per Fernzugriff die Leistung eines Geräts verbessern, indem Sie nicht mehr benötigte Dateien schnell und einfach aufspüren und entfernen. Klicken Sie auf **START** und wählen Sie dann die Bereiche aus, die Sie optimieren möchten. Klicken Sie erneut auf **START**, um den Optimierungsvorgang zu starten. Klicken Sie auf **Weitere Details**, um einen detaillierten Bericht mit Informationen zu den behobenen Problemen aufzurufen.
- **Diebstahlschutz.** Falls Sie Ihr Gerät verlegen oder verlieren oder sollte es gestohlen werden, hilft Ihnen die Diebstahlschutzfunktion Ihr Gerät zu orten und per Fernzugriff bestimmte Aktionen durchzuführen. Klicken Sie auf **ORTEN**, um den Standort des Geräts zu ermitteln. Der letzte bekannte Standort wird zusammen mit Uhrzeit und Datum angezeigt.
- **Schwachstelle.** Um ein Gerät auf Schwachstellen wie fehlende Windows-Updates, veraltete Anwendungen oder unsichere Passwörter zu überprüfen, klicken Sie im Reiter Schwachstellen auf **SCANNEN**. Schwachstellen können nicht per Fernzugriff behoben werden. Falls



eine Schwachstelle gefunden wird, müssen Sie einen erneuten Scan auf dem Gerät durchführen und dann die empfohlenen Maßnahmen ergreifen. Klicken Sie auf **Weitere Details**, um einen detaillierten Bericht über die gefundenen Probleme aufzurufen.



2.3.8. 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.

2.4. Bitdefender auf dem neuesten Stand halten

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

Falls Sie über eine Breitbandverbindung oder eine DSL-Verbindung verfügen, arbeitet Bitdefender eigenständig. Die Software sucht standardmäßig nach Updates, wenn Sie Ihr Gerät einschalten und danach einmal pro **Stunde**. Wenn ein neues Update gefunden wird, wird es automatisch auf Ihr Gerät heruntergeladen und installiert.

Der Updatevorgang wird "on the fly" durchgeführt. Das bedeutet, dass die entsprechenden Dateien stufenweise aktualisiert werden. So stört der Updatevorgang 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 Gerät über einen Proxy-Server mit dem Internet verbunden ist, müssen Sie die Proxy-Einstellungen wie unter beschrieben konfigurieren.
- ☐ Wenn Sie über eine Einwahlverbindung mit dem Internet verbunden sind, wird empfohlen, regelmäßig ein manuelles Bitdefender-Update durchzuführen. Weitere Informationen finden Sie unter .

2.4.1. Überprüfen, ob Bitdefender auf dem neuesten Stand ist

So können Sie den Zeitpunkt des letzten Bitdefender-Updates ermitteln:



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

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

2.4.2. Durchführung eines Updates

Sie benötigen eine Internet-Verbindung, um Updates durchzuführen.

Rechtsklicken Sie zum Start eines Updates in der **Taskleiste** 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

Es kann erforderlich sein, das Gerät nach Abschluss des Updates neu zu starten. 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 einem Windows-Gerät aktualisieren:

1. Zugang [Bitdefender-Zentrale](#).
2. Wähle aus **Meine Geräte** Tafel.
3. Klicken Sie auf die gewünschte Gerätekarte und dann auf die  Symbol in der oberen rechten Ecke des Bildschirms.
4. Wählen **Aktualisieren**.

2.4.3. Aktivieren / Deaktivieren der automatischen Updates

So können Sie automatische Updates aktivieren oder deaktivieren:



1. Klicken **Einstellungen** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Wechseln Sie zum Reiter **Update**.
3. Aktivieren oder deaktivieren Sie den entsprechenden Schalter.
4. Ein Warnung wird angezeigt. Sie müssen Ihre Auswahl bestätigen, indem Sie im Menü wählen, wie lange die automatischen Updates deaktiviert bleiben sollen.
Sie können automatische Updates für 5, 15 oder 30 Minuten, 1 Stunde oder bis zum Neustart des Systems deaktivieren.



Warnung

Hierbei handelt es sich um ein grobes Sicherheitsrisiko. Wir empfehlen die Deaktivierungszeit so gering wie möglich zu halten da BitDefender Sie nur gegen die neusten Bedrohungen schützen kann wenn dieser aktuell ist.

2.4.4. Update-Einstellungen anpassen

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

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

So können Sie die Update-Einstellungen anpassen:

1. Klicken **Einstellungen** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
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-Verarbeitungsregeln

Sobald ein Update verfügbar ist, lädt Bitdefender es automatisch herunter und installiert es, ohne Sie vorher zu benachrichtigen. Deaktivieren Sie



die Option **Update im Hintergrund**, wenn Sie über die Verfügbarkeit neuer Updates benachrichtigt werden möchten.

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 das Gerät aus eigenen Stücken neu startet. Dadurch soll verhindert werden, dass der Update-Prozess von Bitdefender den Benutzer in seiner Arbeit behindert.

Wenn Sie nach einem Update über die Notwendigkeit eines Neustarts informiert werden möchten, aktivieren Sie die **Neustartbenachrichtigung**.

2.4.5. Regelmäßige Updates

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

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



Notiz

Die Updates mit neuen Funktionen und Verbesserungen sind Benutzern vorbehalten, bei denen Bitdefender 2020 installiert ist.



3. VERWALTEN IHRER SICHERHEIT

3.1. Virenschutz

Bitdefender schützt Ihr Gerät vor allen Arten von Bedrohungen (Malware, Trojaner, Spyware, Rootkits etc.). Der Virenschutz ist in zwei Kategorien aufgeteilt:

- **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 Gerät 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 eine klassische, durch den Benutzer gestartete, Prüfung - Sie wählen das Laufwerk, Ordner oder Datei welche BitDefender prüfen soll, und BitDefender prüft diese.

Bitdefender scannt automatisch alle Wechselmedien, die mit dem Gerät verbunden werden, um einen sicheren Zugriff zu garantieren. Weitere Informationen finden Sie im Kapitel [Automatischer Scan von Wechselmedien \(Seite 62\)](#).

Erfahrene Benutzer können Scan-Ausnahmen konfigurieren, wenn Sie nicht möchten, dass bestimmte Dateien oder Dateitypen gescannt werden. Weitere Informationen finden Sie im Kapitel [Konfigurieren der Scan-Ausnahmen \(Seite 64\)](#).

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 \(Seite 67\)](#).

Wenn Ihr Gerät durch Bedrohungen infiziert wurde, siehe [Entfernung von Bedrohungen \(Seite 108\)](#). Um Ihnen bei der Entfernung von Bedrohungen zu helfen, die nicht von innerhalb des Windows-Betriebssystems entfernt werden können, erhalten Sie mit Bitdefender eine [Rettungsumgebung](#). Dabei handelt es sich um eine vertrauenswürdige Umgebung, die speziell der Entfernung von Bedrohungen dient und es Ihnen ermöglicht, Ihr Gerät unabhängig von Windows zu starten. Wenn das Gerät in der Rettungsumgebung ausgeführt wird, sind die Windows-Bedrohungen inaktiv, so dass sie leicht entfernt werden können.

3.1.1. Zugriff-Scans (Echtzeitschutz)

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

Aktivieren / Deaktivieren des Echtzeitschutzes

So können Sie den Echtzeitschutz vor Bedrohungen aktivieren oder deaktivieren:

1. Klicken Sie im Navigationsmenü der **Bitdefender-Benutzeroberfläche** auf **Schutz**.
2. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Öffnen**.
3. Aktivieren oder deaktivieren Sie im Fenster **Erweitert** die Option **Bitdefender-Schild**.
4. Wenn Sie den Echtzeitschutz deaktivieren, wird ein Warnfenster angezeigt. Sie müssen Ihre Auswahl bestätigen, indem Sie im Menü wählen, wie lange der Echtzeitschutz deaktiviert bleiben soll. Sie können den Echtzeitschutz für 5, 15 oder 30 Minuten, 1 Stunde, dauerhaft oder bis zum Neustart des Systems deaktivieren. Der Echtzeitschutz wird automatisch nach Ablauf des festgelegten Zeitraums aktiviert.



Warnung

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



Erweiterte Einstellungen des Echtzeitschutzes konfigurieren

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

So können Sie die erweiterten Einstellungen für den Echtzeitschutz konfigurieren:

1. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Im Fenster **Erweitert** können Sie die Scan-Einstellungen nach Bedarf konfigurieren.

Informationen zu den Scan-Optionen

Diese Informationen sind vielleicht nützlich:

- **Nur Anwendungen scannen.** Sie können Bitdefender so einrichten, dass nur aufgerufene Anwendungen gescannt werden.
- **Auf potenziell unerwünschte Anwendungen prüfen.** Aktivieren Sie diese Option, um nach nicht erwünschten Anwendungen zu suchen. Bei einer potenziell unerwünschten Anwendung (PUA) oder einem potenziell unerwünschten Programm (PUP) handelt es sich um Software, die meist in Verbindung mit kostenloser Software installiert wird und danach Pop-up-Nachrichten anzeigt oder eine Symbolleiste im Standard-Browser installiert. Einige dieser Anwendungen und Programme verändern die Homepage oder die Suchmaschine, andere führen Hintergrundprozesse aus, die den PC verlangsamen, oder zeigen immer wieder Werbung an. Diese Programme können ohne Ihre Zustimmung installiert werden (wird auch als Adware bezeichnet) oder werden standardmäßig bei der Express-Installation mitinstalliert (werbeunterstützt).
- **Auf Skripte scannen.** Die Funktion Auf Skripte scannen erlaubt es Bitdefender, PowerShell-Skripte und Office-Dokumente zu scannen, die skriptbasierte Malware enthalten können.
- **Netzwerkfreigaben scannen.** Um von Ihrem Gerät aus sicher auf Remotenetzezugreifen zu können, empfehlen wir die Option Netzwerkfreigaben scannen aktiviert zu lassen.



- **Prozessspeicher scannen.** Sucht nach schädlichen Aktivitäten im Speicher von laufenden Prozessen.
- **Befehlszeile scannen.** Scant die Befehlszeile von neu gestarteten Anwendungen, um dateilose Angriffe zu verhindern.
- **Archive scannen.** Das Scannen von Archiven ist ein langsamer und ressourcenintensiver Prozess und wird daher nicht für den Echtzeitschutz empfohlen. Archive, die infizierte Dateien enthalten, stellen keine unmittelbare Bedrohung für die Sicherheit Ihres Systems dar. Die Bedrohung kann Ihr System nur dann beeinträchtigen, wenn die infizierte Datei aus dem Archiv extrahiert und dann ohne aktivierten Echtzeitschutz ausgeführt wird.
Wenn Sie sich für diese Option entscheiden, aktivieren Sie sie und ziehen Sie den Regler dann entlang der Skala, um Archive, die größer als ein bestimmter Wert in MB (Megabyte) sind, vom Scan auszuschließen.
- **Boot-Sektoren scannen.** Sie können Bitdefender so einrichten, dass die Boot-Sektoren Ihrer Festplatte gescannt werden. Dieser Sektor der Festplatte enthält den notwendigen Computercode, um den Boot-Vorgang zu starten. Wenn eine Bedrohung den Boot-Sektor infiziert, kann das Laufwerk unzugänglich werden und Sie können Ihr System nicht mehr starten und auf Ihre Daten zugreifen.
- **Nur neue und veränderte Dateien scannen.** Indem Sie nur neue und geänderte Dateien scannen, können Sie die allgemeine Reaktionsfähigkeit Ihres Systems mit minimalen Einbußen bei der Sicherheit erheblich verbessern.
- **Auf Keylogger prüfen.** Wählen Sie diese Option, um Ihr System auf Keylogger zu prüfen. Keylogger zeichnen auf, was Sie über Ihre Tastatur eingeben, und schicken dann via Internet Berichte an Hacker. Hacker können über diese gestohlenen Daten sensible Informationen erfahren, so wie Kontonummern und Passwörter und Sie zu ihrem eigenen Profit verwenden.
- **Früher Boot-Scan.** Wählen Sie die Option **Füher Boot-Scan**, um Ihr System beim Start zu scannen, sobald alle kritischen Dienste geladen sind. Diese Funktion verbessert die Erkennung von Bedrohungen beim Systemstart und lässt Ihr System schneller starten.



Für gefundene Bedrohungen durchgeführte Aktionen

So können Sie einstellen welche Aktionen der Echtzeitschutz durchführen soll:

1. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Scrollen Sie im Fenster **Erweitert** nach unten, bis Sie die Option **Bedrohungsaktionen** sehen.
4. 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 in der Bitdefender-Datenbank gefundenen Bedrohungsinformationen überein. Bitdefender wird automatisch versuchen, den Schadcode aus der infizierten Datei zu entfernen und die Originaldatei zu rekonstruieren. Diesen Vorgang 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 \(Seite 67\)](#).



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 Labs 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.

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 \(Seite 67\)](#).

Zugriff verweigern

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

Wiederherstellen der Standardeinstellungen

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

Um die vorgegebenen Echtzeitschutz-Einstellungen wiederherzustellen:

1. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Scrollen Sie im Fenster **Erweitert** nach unten, bis Sie die Option **Erweiterte Einstellungen zurücksetzen** sehen. Wählen Sie diese Option aus, um die Virenschutzeinstellungen auf die Standardeinstellungen zurückzusetzen.

3.1.2. Bedarf-Scan

Die Aufgabe der Bitdefender-Software ist es sicherzustellen, dass es keine Bedrohungen auf Ihrem Gerät gibt. Dies wird erreicht, indem



neue Bedrohungen ferngehalten und Ihre E-Mail-Nachrichten sowie alle heruntergeladenen oder auf Ihr Gerät 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 Ihr Gerät nach der Installation von Bitdefender auf bereits vorhandene Bedrohungen prüfen. Übrigens sollten Sie Ihr Gerät 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 das Gerät jederzeit scannen, indem Sie die Standard-Aufgaben oder Ihre eigenen Scan-Aufgaben (benutzerdefinierte Aufgaben) ausführen. Wenn Sie bestimmte Bereiche Ihres Geräts scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierten Scan konfigurieren und ausführen.

Eine Datei oder einen Ordner auf Bedrohungen prüfen

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

Durchführen von Quick Scans

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

So können Sie eine Quick Scan durchführen:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.



3. Klicken Sie im Fenster **Scans** neben **Quick Scan** auf die Schaltfläche **Scan starten**.
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.

Durchführen von System-Scans

Der System-Scan prüft das gesamte Gerät auf alle Bedrohungsarten, die ein Sicherheitsrisiko darstellen, so zum Beispiel Malware, Spyware, Adware, Rootkits usw.



Notiz

Da ein **System-Scan** das gesamte System scannt, kann er eine Weile dauern. Es empfiehlt sich daher, diese Aufgabe durchzuführen, wenn Sie das Gerät gerade 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 \(Seite 43\)](#).
- Schließen Sie alle geöffneten Programme.

Wenn Sie bestimmte Bereiche Ihres Geräts scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierten Scan konfigurieren und ausführen. Weitere Informationen finden Sie im Kapitel [Benutzerdefinierte Scans durchführen \(Seite 55\)](#).

So können Sie einen System-Scan durchführen:

1. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Klicken Sie im Fenster **Scans** neben **System-Scan** auf die Schaltfläche **Scan starten**.



4. Bei der ersten Durchführung eines System-Scans werden Sie mit der Funktion vertraut gemacht. Klicken zum Fortfahren auf **OK, verstanden**.
5. Folge dem [Antivirus-Scan-Assistent](#) um den Scan abzuschließen. Bitdefender ergreift automatisch die empfohlenen Maßnahmen für erkannte Dateien. Wenn es weiterhin ungelöste Bedrohungen gibt, werden Sie aufgefordert, die Maßnahmen auszuwählen, die für sie ergriffen werden sollen.

Benutzerdefinierte Scans durchführen

Im Fenster **Scans verwalten** können Sie Bitdefender so einrichten, dass Scans ausgeführt werden, wenn Sie glauben, dass Ihr Gerät eine Überprüfung auf mögliche Bedrohungen benötigt. Sie können wählen, ob Sie einen **System-Scan** oder einen **Quick-Scan** planen möchten, oder ob Sie einen benutzerdefinierten Scan nach Ihren Anforderungen erstellen möchten.

So können Sie einen benutzerdefinierten Scan im Detail konfigurieren:

1. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Klicken Sie im Fenster **Scans** auf **+Scan erstellen**.
4. Geben Sie im Feld **Aufgabenname** einen Namen für den Scan ein, wählen Sie die Bereiche aus, die Sie scannen möchten, und klicken Sie auf **Weiter**.
5. Konfigurieren Sie diese allgemeinen Optionen:
 - ☐ **Nur Anwendungen scannen**. Sie können Bitdefender so einstellen, dass nur aufgerufene Apps gescannt werden.
 - ☐ **Priorität der Scan-Aufgabe**. Sie können festlegen, wie sich ein Scan-Vorgang auf die Systemleistung auswirkt.
 - ☐ **Auto** - Die Priorität des Scan-Vorgangs hängt von der Systemaktivität ab. Um sicherzustellen, dass der Scan-Vorgang die Systemaktivität nicht beeinträchtigt, entscheidet Bitdefender, ob der Scan-Vorgang mit hoher oder niedriger Priorität ausgeführt wird.
 - ☐ **Hoch** - Die Priorität des Scan-Vorgangs wird als hoch festgelegt. Wenn Sie diese Option wählen, können andere Programme



langsamer ausgeführt werden. So kann der Scan-Vorgang schneller abgeschlossen werden.

- ☐ Niedrig - Die Priorität des Scan-Vorgangs wird als niedrig festgelegt. Wenn Sie diese Option wählen, können andere Programme schneller ausgeführt werden. So dauert es länger, bis der Scan-Vorgang abgeschlossen wird.
 - ☐ **Aktionen nach dem Scan.** Wählen Sie die Aktion, die von Bitdefender durchgeführt werden soll, wenn keine Bedrohungen gefunden wurden:
 - ☐ Übersichtsfenster anzeigen
 - ☐ Gerät herunterfahren
 - ☐ Scan-Fenster schließen
6. Um die Scan-Optionen im Detail zu konfigurieren, klicken Sie auf **Erweiterte Optionen anzeigen**. Informationen zu den aufgeführten Scans finden Sie am Ende dieses Abschnitts. Klicken Sie auf **Weiter**.
7. Sie können bei Bedarf die Option **Scan-Aufgabe planen** aktivieren und dann festlegen, wann der von Ihnen erstellte benutzerdefinierte Scan gestartet werden soll.
- ☐ Beim Systemstart
 - ☐ Täglich
 - ☐ Monatlich
 - ☐ Wöchentlich

Wenn Sie Täglich, Monatlich oder Wöchentlich wählen, ziehen Sie den Regler entlang der Skala, um den gewünschten Zeitraum festzulegen, in dem der geplante Scan beginnen soll.

8. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Konfigurationsfenster zu schließen.
- Abhängig von den Bereichen, die gescannt werden sollen, kann der Scan einige Zeit in Anspruch nehmen. Wenn während des Scan-Vorgangs Bedrohungen gefunden werden, werden Sie aufgefordert, die Aktionen auszuwählen, die für die erkannten Dateien durchgeführt werden sollen.



Informationen zu den Scanoptionen

Sie können diese Informationen nützlich finden:

- Wenn Ihnen bestimmte Begriffe nicht geläufig sind, schlagen Sie diese im **Glossar** nach. Sie können auch durch eine Suche im Internet hilfreiche Informationen finden.
- **Scannen Sie potenziell unerwünschte Anwendungen.** Wählen Sie diese Option, um nach unerwünschten Anwendungen zu suchen. Eine potenziell unerwünschte Anwendung (PUA) oder ein potenziell unerwünschtes Programm (PUP) ist eine Software, die normalerweise mit Freeware-Software gebündelt geliefert wird und im Standardbrowser Popups anzeigt oder eine Symbolleiste installiert. Einige von ihnen ändern die Startseite oder die Suchmaschine, andere führen mehrere Prozesse im Hintergrund aus, die den PC verlangsamen, oder zeigen zahlreiche Anzeigen an. Diese Programme können ohne Ihre Zustimmung installiert werden (auch als Adware bezeichnet) oder sind standardmäßig im Express-Installationskit enthalten (werbefinanziert).
- **Archive scannen.** Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für Ihre Systemsicherheit. Archive, die infizierte Dateien enthalten, stellen keine unmittelbare Bedrohung für die Sicherheit Ihres Systems dar. Die Bedrohung kann Ihr System nur dann beeinträchtigen, wenn die infizierte Datei aus dem Archiv extrahiert und dann ohne aktivierten Echtzeitschutz ausgeführt wird. Wir empfehlen jedoch, diese Option zu nutzen, um potenzielle Bedrohungen aufzuspüren und zu entfernen, auch wenn es sich nicht um unmittelbare Bedrohungen handelt.
Ziehen Sie den Regler entlang der Skala, um Archive, die größer als ein bestimmter Wert in MB (Megabyte) sind, vom Scan auszuschließen.



Notiz

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

- **Scannen Sie nur neue und geänderte Dateien.** Indem Sie nur neue und geänderte Dateien scannen, können Sie die Reaktionsfähigkeit des Gesamtsystems mit einem minimalen Kompromiss bei der Sicherheit erheblich verbessern.



- **Bootsektoren scannen.** Sie können Bitdefender so einstellen, dass es die Bootsektoren Ihrer Festplatte scannt. Dieser Sektor der Festplatte enthält den notwendigen Computercode, um den Startvorgang zu starten. Wenn eine Bedrohung den Bootsektor infiziert, kann das Laufwerk unzugänglich werden und Sie können Ihr System möglicherweise nicht starten und nicht auf Ihre Daten zugreifen.
- **Speicher scannen.** Wählen Sie diese Option, um Programme zu scannen, die im Speicher Ihres Systems laufen.
- **Registrierung scannen.** Wählen Sie diese Option, um die Registrierungsschlüssel 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 Browsern auf Ihrem Gerät gespeichert werden.
- **Keylogger scannen.** Wählen Sie diese Option, um Ihr System nach Keylogger-Apps zu durchsuchen. Keylogger zeichnen auf, was Sie auf Ihrer Tastatur eingeben, und senden Berichte über das Internet an eine böswillige Person (Hacker). Der Hacker kann aus den gestohlenen Daten sensible Informationen wie Bankkontonummern und Passwörter herausfinden und daraus persönliche Vorteile ziehen.

Viren-Scan-Assistent

Wenn 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-Vorgang abzuschließen.



Notiz

Falls der Scan-Assistent nicht erscheint, ist der Scan möglicherweise als Hintergrund-Scan konfiguriert. Suchen Sie nach dem Symbol für den Scan-Fortschritt **B** in der **Taskleiste**. Klicken Sie auf das Symbol, um das Scan-Fenster zu öffnen und so den Scan-Fortschritt zu sehen.

Schritt 1 - Führen Sie den Scan durch

BitDefender prüft die gewählten Dateien und Ordner. 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 Prüfvorgang 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 unterbrechen, indem Sie auf **STOPP** klicken. Sie gelangen dann direkt zum letzten Schritt des Assistenten. Um den Scan-Vorgang nur vorübergehend anzuhalten, klicken Sie einfach auf **PAUSE**. Klicken Sie auf **FORTSETZEN**, um den Scan-Vorgang fortzusetzen.

Passwortgeschützte Archive. Wird ein passwortgeschütztes Archiv gefunden, werden Sie abhängig von den Scan-Einstellungen zur Eingabe des Passworts aufgefordert. Passwortgeschützte Archive können nur nach Eingabe des Passworts gescannt werden. 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 einem Passwort fragen und dieses Objekt beim Scan überspringen.** Wählen Sie diese Option, um das Scannen dieses Archivs zu überspringen.
- ☐ **Alle passwortgeschützten Dateien beim Scan überspringen.** Wählen Sie diese Option, falls Sie nicht über passwortgeschützte Archive informiert werden möchten. Bitdefender kann diese dann 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.



Notiz

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 ergreift je nach Typ der erkannten Datei die empfohlenen Maßnahmen:

- **Infizierte Dateien.** Als infiziert erkannte Dateien stimmen mit Bedrohungsinformationen überein, die in der Bitdefender-Datenbank für Bedrohungsinformationen gefunden wurden. Bitdefender versucht automatisch, den Schadcode aus der infizierten Datei zu entfernen und die Originaldatei zu rekonstruieren. Dieser Vorgang wird als Desinfektion bezeichnet.

Dateien, die nicht desinfiziert werden können, werden in die Quarantäne verschoben, um die Infektion einzudämmen. Quarantänedateien können nicht ausgeführt oder geöffnet werden; daher verschwindet das Risiko, sich zu infizieren. Weitere Informationen finden Sie unter [Verwalten von Dateien in Quarantäne \(Seite 67\)](#).

Wichtig

Bei bestimmten Arten von Bedrohungen ist eine Desinfektion nicht möglich, da die erkannte Datei vollständig bösartig ist. In solchen Fällen wird die infizierte Datei von der Festplatte gelöscht.

- **Verdächtige Dateien.** Dateien werden von der heuristischen Analyse als verdächtig erkannt. Verdächtige Dateien können nicht desinfiziert werden, da keine Desinfektionsroutine verfügbar ist. Sie werden in Quarantäne gebracht, um eine mögliche Ansteckung zu verhindern. Dateien in Quarantäne werden standardmäßig an die Bitdefender Labs 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 saubere Dateien enthält, versucht Bitdefender, die infizierten Dateien zu löschen, sofern es das Archiv mit den sauberen Dateien rekonstruieren kann. Wenn die Wiederherstellung des Archivs nicht möglich ist, werden Sie darüber informiert, dass keine Maßnahmen ergriffen werden können, um den Verlust sauberer Dateien zu vermeiden.

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 durchführen

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 das Beheben der Risiken beendet hat wird eine Zusammenfassung in einem neuen Fenster geöffnet. Falls Sie umfangreichere Informationen zum Scan-Prozess möchten, klicken Sie auf **LOGDATEI ANZEIGEN**.



Wichtig

In den meisten Fällen desinfiziert BitDefender erfolgreich die infizierten Dateien, die er entdeckt hat, 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](#) (Seite 108).

3.1.3. 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 **Benachrichtigungen** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
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**.

3.1.4. Automatischer Scan von Wechselmedien

Bitdefender erkennt automatisch, wenn Sie Wechselmedien mit Ihrem Gerät verbinden und scannt diese im Hintergrund, wenn die Auto-Scan-



Option aktiviert wurde. Dies ist empfohlen, um die Infizierung Ihres Geräts durch Bedrohungen zu verhindern.

Entdeckte Geräte fallen in eine dieser Kategorien:

- CDs/DVDs
- Speichersticks, wie z. B. Flash Pens oder externe Festplatten
- verbundene (entfernte) Netzlaufwerke

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

Wie funktioniert es?

Wenn ein Wechseldatenträger erkannt wird, beginnt Bitdefender diesen auf Bedrohungen zu prüfen (vorausgesetzt, dass der automatische Scan für diesen Gerätetyp aktiviert ist). Ein Pop-up-Fenster wird Sie darüber informieren, dass ein neues Gerät erkannt wurde und dass es derzeit gescannt wird.

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.

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.

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.



Notiz

Bitte beachten Sie, dass für infizierte oder verdächtige Dateien auf CDs oder DVDs keine Aktionen durchgeführt werden können. Ebenso können für infizierte oder verdächtige Dateien auf abgebildeten Netzlaufwerken keine Aktionen durchgeführt werden, wenn Sie nicht die über die entsprechenden Rechte verfügen.

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 \(Seite 108\)](#).

Verwalten des Scans für Wechselmedien

So können Sie Wechselmedien automatisch scannen:

1. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Rufen Sie das Fenster **Einstellungen** auf.

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.

Um den bestmöglichen Schutz zu garantieren, empfiehlt es sich, die **Auto-Scan-Option** für alle Arten von Wechselmedien zu aktivieren.

3.1.5. Konfigurieren der Scan-Ausnahmen

Mit Bitdefender können Sie bestimmte Dateien, Ordner oder Dateieindungen vom Scan ausnehmen. Diese Funktion soll verhindern, dass Sie bei Ihrer Arbeit gestört werden und kann zudem dabei helfen, die Systemleistung zu verbessern. Ausnahmen sollten nur von Benutzern eingesetzt werden, die erfahren im Umgang mit Computern sind oder wenn dies von einem Bitdefender-Mitarbeiter empfohlen wurde.

Sie können Ausnahmen 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.



Notiz

Ausnahmen werden bei Kontext-Scans NICHT berücksichtigt. Kontextprüfung ist eine Art von On-Demand-Prüfung: rechtsklicken Sie die zu prüfende Datei oder den Ordner und wählen Sie **Prüfe mit BitDefender** aus.

Dateien und Ordner vom Scan ausnehmen

So können Sie bestimmte Dateien und Ordner vom Scan ausnehmen:

1. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Klicken Sie im Fenster **Einstellungen** auf **Ausnahmen verwalten**.
4. Klicken Sie auf **+Ausnahme hinzufügen**.
5. Geben Sie den Pfad des Ordners, den Sie vom Scan ausnehmen möchten, in das entsprechende Feld ein.
Alternativ können Sie zu dem Ordner navigieren, indem Sie rechts in der Benutzeroberfläche auf die Schaltfläche "Durchsuchen" klicken, ihn auswählen und dann auf **OK** klicken.
6. Aktivieren Sie den Schalter neben der Schutzfunktion, durch die der Ordner nicht gescannt werden soll. Sie haben drei Optionen:
 - ☐ Virenschutz
 - ☐ Online-Gefahrenabwehr
 - ☐ Erweiterte Gefahrenabwehr
7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Fenster zu schließen.

Dateiendungen vom Scan ausnehmen

Wenn Sie eine Dateiendung vom Scan ausnehmen, wird Bitdefender Dateien mit dieser Endung unabhängig von ihrem Speicherort nicht mehr scannen. Die Ausnahme bezieht sich auch auf Dateien auf Wechselmedien, wie zum Beispiel CDs, DVDs, USB-Sticks oder Netzlaufwerke.



Wichtig

Lassen Sie Vorsichtig walten, wenn Sie Dateiendung vom Scan ausnehmen, da solche Ausnahmen Ihr Gerät anfällig für Bedrohungen machen können.

So können Sie Dateierweiterungen vom Scan ausnehmen:

1. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Im **Einstellungen** Fenster, klicken **Ausnahmen verwalten**.
4. Klicken **+Fügen Sie eine Ausnahme hinzu**.
5. Geben Sie die Dateiendungen, die vom Scannen ausgenommen werden sollen, mit einem Punkt davor ein. Trennen Sie einzelne Endungen mit einem Semikolon (;).
txt;avi;jpg
6. Aktivieren Sie den Schalter neben der Schutzfunktion, durch die die Dateiendung nicht gescannt werden soll.
7. Klicken Sie auf **Speichern**.

Verwalten der Scan-Ausnahmen

Werden die konfigurierten Scan-Ausnahmen nicht mehr benötigt, empfehlen wir, diese zu löschen oder die Scan-Ausnahmen zu deaktivieren.

So können Sie die Scan-Ausnahmen verwalten:

1. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Klicken Sie im Fenster **Einstellungen** auf **Ausnahmen verwalten**. Es wird eine Liste mit allen von Ihnen festgelegten Ausnahmen angezeigt.
4. Um Scan-Ausnahmen zu entfernen oder zu bearbeiten, klicken Sie auf die jeweiligen Schaltflächen. Gehen Sie wie folgt vor:
 - Entfernen Sie einen Eintrag aus der Liste, indem Sie auf die entsprechende -Schaltfläche klicken.
 - Klicken Sie zum Bearbeiten eines Eintrags aus der Tabelle auf die Schaltfläche **Bearbeiten** neben dem Eintrag. Ein neues Fenster wird angezeigt. Hier können Sie nach Bedarf festlegen, welche Dateiendungen oder -pfade von welcher Schutzfunktion



ausgeschlossen werden sollen. Führen Sie die notwendigen Änderungen durch und klicken Sie dann auf **Ändern**.

3.1.6. Verwalten von Dateien in Quarantäne

Mit Bedrohungen infizierte Dateien, die nicht desinfiziert werden können, sowie verdächtige Dateien werden von Bitdefender in einem sicheren Bereich isoliert, der sogenannten Quarantäne. Bedrohungen in Quarantäne können keinen Schaden anrichten, da sie dort nicht geöffnet oder ausgeführt werden können.

Standardmäßig werden isolierte Dateien automatisch an die Bitdefender-Labs gesendet, damit sie von den Bitdefender-Bedrohungsforschern analysiert werden. Wenn das Vorhandensein einer Bedrohung bestätigt wird, wird eine Informationsaktualisierung veröffentlicht, um das Entfernen der Bedrohung zu ermöglichen.

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 **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Rufen Sie das Fenster **Einstellungen** auf.
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 Bedrohungsinformationen 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.

Inhalte löschen, die älter als 30 Tage sind

Dateien in Quarantäne, die älter als 30 Tage sind, werden automatisch gelöscht.

Ausnahmen 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 Quarantäne-Datei zu löschen, markieren Sie diese und klicken dann auf den Button **Löschen**. Wenn Sie eine Quarantäne-Datei am ursprünglichen Speicherort wiederherstellen möchten, klicken Sie zuerst auf die Datei und dann auf **Wiederherstellen**.

3.2. Erweiterte Bedrohungsabwehr

Die Erweiterte Gefahrenabwehr von Bitdefender 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 Gerät laufenden Anwendungen auf Aktionen, die auf Bedrohungen hindeuten. Jede einzelne dieser Aktionen erhält einen Wert, und jeder Prozess erhält so einen aggregierten Gesamtwert.

Als Sicherheitsmaßnahme werden Sie jedes Mal benachrichtigt, wenn Bedrohungen und potenziell gefährliche Prozesse erkannt und blockiert werden.

3.2.1. Aktivieren oder Deaktivieren der Advanced Threat Defense

So aktivieren oder deaktivieren Sie die Advanced Threat Defense:

1. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Klicken Sie im Bereich **ERWEITERTE GEFAHRENABWEHR** auf **Öffnen**.
3. Rufen Sie das Fenster **Einstellungen** auf und klicken Sie auf den Schalter neben **Bitdefender Erweiterte Gefahrenabwehr**.



Notiz

Zum Schutz Ihrer Systeme vor Ransomware und anderen Bedrohungen empfehlen wir Ihnen, die Erweiterte Gefahrenabwehr nicht über einen längeren Zeitraum zu deaktivieren.

3.2.2. Einsehen von erkannten schädlichen Angriffen

Werden Bedrohungen oder potenziell schädliche Angriffe erkannt, werden diese von Bitdefender umgehend blockiert, um eine Infektion Ihres Geräts durch Ransomware oder andere Malware zu verhindern. Gehen Sie wie folgt vor, um eine Liste der erkannten schädlichen Angriffe einzusehen:

1. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Im **ERWEITERTE BEDROHUNGSABWEHR** Bereich, klicken Sie auf **Offen**.
3. Rufen Sie das Fenster **Threat Defense** auf.

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.

3.2.3. Hinzufügen von Prozessen zu den Ausnahmen

Sie können Ausnahmeregeln für vertrauenswürdige Anwendungen festlegen, damit die Erweiterte Gefahrenabwehr diese nicht blockiert, wenn ihr Verhalten auf eine Bedrohung hindeutet.

So können Sie Prozesse zur Ausnahmeliste der Erweiterten Gefahrenabwehr hinzufügen:

1. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Im **ERWEITERTE BEDROHUNGSABWEHR** Bereich, klicken Sie auf **Offen**.
3. Im **Einstellungen** Fenster, klicken **Ausnahmen verwalten**.
4. Klicken **+Fügen Sie eine Ausnahme hinzu**.
5. Geben Sie den Pfad des Ordners, den Sie vom Scannen ausnehmen möchten, in das entsprechende Feld ein.

Alternativ können Sie zu der ausführbaren Datei navigieren, indem Sie rechts in der Benutzeroberfläche auf die Schaltfläche "Durchsuchen" klicken, sie auswählen und dann auf **OK** klicken.



6. Aktivieren Sie den Schalter neben **Erweiterte Gefahrenabwehr**.
7. Klicken **Speichern**.

3.2.4. Exploits gefunden

Hacker nutzen zum Eindringen in Systeme häufig bestimmte Fehler oder Schwachstellen in Computersoftware (Anwendungen oder Plug-ins) und Hardware aus. Um Ihr Gerät von derartigen Angriffen zu schützen, die sich in aller Regel sehr schnell ausbreiten, verwendet Bitdefender die neuesten Technologien zur Abwehr von Exploits.

3.2.5. Aktivieren oder Deaktivieren der Exploit-Erkennung

So können Sie die Exploit-Erkennung aktivieren oder deaktivieren:

- ☐ Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
- ☐ Im **ERWEITERTE BEDROHUNGSABWEHR** Bereich, klicken Sie auf **Offen**.
- ☐ Rufen Sie das Fenster **Einstellungen** auf und klicken Sie auf den Schalter neben **Exploit-Erkennung**, um die Funktion zu aktivieren oder deaktivieren.



Notiz

Die Option zur Exploit-Erkennung ist standardmäßig aktiviert.

3.3. Abwehr von Online-Bedrohungen

Die Online-Gefahrenabwehr von Bitdefender lässt Sie sicher im Netz surfen, indem sie Sie vor potenziell schädlichen Seiten warnt.

Bitdefender bietet Echtzeit-Online-Gefahrenabwehr für:

- ☐ Internet Explorer
- ☐ Microsoft Edge
- ☐ Mozilla Firefox
- ☐ Google Chrome
- ☐ Safari
- ☐ Bitdefender Safepay™
- ☐ Opera



So können Sie die Einstellungen der Online-Gefahrenabwehr konfigurieren:

1. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Klicken Sie im Bereich **ONLINE-GEFAHRENABWEHR** auf **Einstellungen**.

Klicken Sie im Bereich **Internet-Schutz** zur Aktivierung oder Deaktivierung auf die entsprechenden Schalter:

- ☐ Die Prävention von Internetangriffen 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. Lassen Sie Vorsicht walten, wenn Sie sie dennoch aufrufen möchten.

 Diese Seite ist sicher und kann aufgerufen werden.

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
- ☐ Verschlüsselter Web-Scan.
Gute durchdachte Angriffsversuche könnten den sicheren Datenverkehr für sich zu nutzen, um ihre Opfer zu täuschen. Wir empfehlen daher, die Option Verschlüsselter Web-Scan aktiviert zu lassen.
- ☐ Betrugsschutz.
- ☐ Phishing-Schutz.

Scrollen Sie nach unten, um zum Abschnitt **Netzwerk-Gefahrenabwehr** zu gelangen. Hier finden Sie die Option **Netzwerk-Gefahrenabwehr**. Um



Ihr Gerät vor Angriffen durch komplexe Malware-Bedrohungen (so z. B. Ransomware) zu schützen, die sich Schwachstellen im System zu Nutze machen, sollten Sie diese Option aktiviert lassen.

Sie können eine Liste mit Websites, Domains und IP-Adressen anlegen, die von den Bitdefender-Engines für den Bedrohungs-, Phishing- und Betrugsschutz nicht gescannt werden sollen. Die Liste sollte nur Websites, Domänen und IP-Adressen enthalten, denen Sie uneingeschränkt vertrauen.

So können Sie mit der Online-Gefahrenabwehr in Bitdefender Websites, Domains und IP-Adressen konfigurieren und verwalten:

1. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Im **VORBEUGUNG VON ONLINE-BEDROHUNGEN** Bereich, klicken Sie auf **Einstellungen**.
3. Klicken Sie auf **Ausnahmen verwalten**.
4. Klicken **+Fügen Sie eine Ausnahme hinzu**.
5. Geben Sie in das entsprechende Feld den Namen der Website, den Namen der Domain oder die IP-Adresse ein, die Sie zu den Ausnahmen hinzufügen möchten.
6. Klicken Sie auf den Schalter neben **Online-Gefahrenabwehr**.
7. Um einen Eintrag aus der Liste zu entfernen, klicken Sie auf  Schaltfläche daneben.
Klicken **Speichern** um die Änderungen zu speichern und das Fenster zu schließen.

3.3.1. 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 stehen Ihnen zur Auswahl:

- ☐ Verlassen Sie die Website mit einem Klick auf **ICH GEHE LIEBER AUF NUMMER SICHER**.



- Rufen Sie die Website trotz der Warnung auf, indem Sie auf **Ich bin mir der Risiken bewusst und möchte trotzdem fortfahren** klicken.
- Wenn Sie sich sicher sind, dass die erkannte Website sicher ist, klicken Sie auf **SENDEN**, um Sie zu den Ausnahmen hinzuzufügen. Wir empfehlen Ihnen, nur Websites hinzuzufügen, denen Sie uneingeschränkt vertrauen.



4. GEWUSST WIE

4.1. Installation

4.1.1. Wie kann ich Bitdefender auf einem zweiten Gerät installieren?

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 Gerät installieren:

1. Klicken Sie unten rechts in der **Bitdefender-Benutzeroberfläche** auf **Auf weiterem Gerät installieren**.
Ein neues Fenster erscheint auf Ihrem Bildschirm.
2. Klicken **DOWNLOAD-LINK TEILEN**.
3. Folgen Sie den angezeigten Anleitung, um Bitdefender zu installieren.

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

4.1.2. Wie kann ich Bitdefender erneut 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 wie folgt vor:

- ☐ In **Windows 7**:
 1. Klicken **Start** und gehe zu **Alle Programme**.
 2. Suchen Sie nach *Bitdefender Antivirus Free* und wählen Sie **Deinstallieren**.



3. Klicken Sie im angezeigten Fenster auf **NEU INSTALLIEREN**.
 4. Sie müssen das Gerät 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. Finden **Bitdefender Antivirus Free** und auswählen **Deinstallieren**.
 4. Klicken **NEU INSTALLIEREN** im erscheinenden Fenster.
 5. Sie müssen das Gerät neu starten, um den Vorgang abzuschließen.
- In **Windows 10 Und Windows11**:
1. Klicken Sie auf **Start** und danach auf **Einstellungen**.
 2. Klicken Sie in den Einstellungen auf das **System**-Symbol und wählen Sie dann **Apps & Funktionen**.
 3. Finden **Bitdefender Antivirus Free** und auswählen **Deinstallieren**.
 4. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.
 5. Klicken Sie auf **ERNEUT INSTALLIEREN**.
 6. Sie müssen das Gerät neu starten, um den Vorgang abzuschließen.



Notiz

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.

4.1.3. Woher kann ich mein Bitdefender-Produkt herunterladen?

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



Notiz

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

So können Sie Bitdefender über Bitdefender Central installieren:

1. Zugang [Bitdefender-Zentrale](#).
2. Wähle aus **Meine Geräte** Panel, und klicken Sie dann auf **SCHUTZ INSTALLIEREN**.
3. Wählen Sie eine der beiden verfügbaren Optionen:

☐ **Schützen Sie dieses Gerät**

Wählen Sie diese Option und dann den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, klicken Sie auf die entsprechende Schaltfläche.

☐ **Schützen Sie andere Geräte**

Wählen Sie diese Option und dann den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, klicken Sie auf die entsprechende Schaltfläche.

Klicken **DOWNLOADLINK SENDEN**. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **E-MAIL SENDEN**. Beachten Sie, dass der generierte Download-Link nur für die nächsten 24 Stunden gültig ist. Wenn der Link abläuft, müssen Sie einen neuen generieren, indem Sie die gleichen Schritte ausführen.

Überprüfen Sie auf dem Gerät, auf dem Sie Ihr Bitdefender-Produkt installieren möchten, das E-Mail-Konto, das Sie eingegeben haben, und klicken Sie dann auf die entsprechende Download-Schaltfläche.

4. Führen Sie das von Ihnen heruntergeladene Bitdefender aus.

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

Ab sofort ist ein Upgrade auf die neueste Version ohne den manuellen Deinstallations- und Neuinstallationsvorgang 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 2020er-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 den Neustart des Geräts ab.
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: <https://www.bitdefender.com/Downloads/>. Die Aktivierung ist nur mit einem gültigen Abonnement möglich.

4.2. Bitdefender-Zentrale

4.2.1. Wie kann ich mein Bitdefender-Benutzerkonto wechseln?

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

So melden Sie sich mit einem anderen Bitdefender-Konto an:

1. Klicken Sie oben im **Bitdefender-Fenster** auf Ihren Kontonamen.
2. Klicken Sie oben rechts im Bildschirm auf **Konto wechseln**, um das Gerät mit einem anderen Benutzerkonto zu verknüpfen.
3. Geben Sie die E-Mail-Adresse in das entsprechende Feld ein und klicken Sie dann auf **NÄCHSTE**.
4. Geben Sie Ihr Kennwort ein und klicken Sie dann auf **ANMELDEN**.



Notiz

Das Bitdefender-Produkt auf Ihrem Gerät wird entsprechend dem mit Ihrem 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 Abschnitt [Hier wird Ihnen geholfen \(Seite 116\)](#) beschrieben mit dem Bitdefender-Support in Verbindung setzen.

4.2.2. 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. Zugang [Bitdefender-Zentrale](#).
2. Drücke den  Symbol oben rechts auf dem Bildschirm.
3. Klicken Sie im Menü auf **Mein Konto**.
4. Klicken Sie im Slide-Menü auf **Einstellungen**.
5. Deaktivieren Sie die Option **Hilfemeldungen aktivieren/deaktivieren**.

4.2.3. 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:

○ Von dem [Bitdefender-Oberfläche](#):

1. Klicken **Mein Konto** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Klicken Sie oben rechts im Bildschirm auf **Konto wechseln**.
Ein neues Fenster wird angezeigt.
3. Geben Sie Ihre E-Mail-Adresse ein und klicken Sie auf **WEITER**.
Ein neues Fenster erscheint.
4. Klicken **Passwort vergessen?**.



5. Klicken Sie auf **WEITER**.
 6. Überprüfen Sie Ihr E-Mail-Konto, geben Sie den Sicherheitscode ein, den Sie erhalten haben, und klicken Sie dann auf **NÄCHSTE**.
Alternativ können Sie auch klicken **Kennwort ändern** in der E-Mail, die wir Ihnen gesendet haben.
 7. Geben Sie das neue Kennwort ein, das Sie festlegen möchten, und geben Sie es dann erneut ein. Klicken **SPEICHERN**.
- Von Ihrem Webbrowser:
1. Gehe zu: <https://central.bitdefender.com>.
 2. Klicken Sie auf **ANMELDEN**.
 3. Geben Sie Ihre E-Mail-Adresse ein und klicken Sie dann auf **NÄCHSTE**.
 4. Klicken **Passwort vergessen?**.
 5. Klicken **NÄCHSTE**.
 6. 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.

4.2.4. 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. Zugang [Bitdefender-Zentrale](#).
2. Drücke den  Symbol oben rechts auf dem Bildschirm.
3. Klicken Sie im Slide-Menü auf **Sitzungen**.
4. Wählen Sie im Bereich **Aktive Sitzungen** die Option **ABMELDEN** neben dem Gerät, für das Sie die Benutzersitzung beenden möchten.



4.3. Prüfen mit BitDefender

4.3.1. 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, bewegen Sie den Mauszeiger auf Bitdefender und klicken Sie im Menü auf **Mit Bitdefender scannen**.

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 Ihr Gerät kopieren.

4.3.2. Wie scanne ich mein System

So können Sie einen vollständigen System-Scan durchführen:

1. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Klicken Sie neben **System-Scan** auf die Schaltfläche **Scan starten**.
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 .

4.3.3. Wie plane ich einen Scan?

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



So können Sie einen Scan planen:

1. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Klicken Sie unten in der Benutzeroberfläche auf ... neben dem Scan-Typ, den Sie planen möchten, System-Scan oder Quick Scan, und wählen Sie dann **Bearbeiten**.
Alternativ können Sie auch einen individuellen Scan-Typ erstellen, indem Sie neben **Scans verwalten** auf **+Scan erstellen** klicken.
4. Richten Sie den Scan entsprechend Ihrer Anforderungen ein und klicken Sie auf **Weiter**.
5. Markieren Sie das Kästchen neben **Legen Sie fest, für wann Sie diese Aufgabe planen möchten**.
Wählen Sie eine der entsprechenden Optionen, um einen Zeitplan festzulegen:
 - ☐ Beim Systemstart
 - ☐ Täglich
 - ☐ Wöchentlich
 - ☐ Monatlich

Wenn Sie „Täglich“, „Monatlich“ oder „Wöchentlich“ auswählen, ziehen Sie den Schieberegler entlang der Skala, um den gewünschten Zeitraum festzulegen, in dem der geplante Scan beginnen soll.

Wenn Sie einen neuen benutzerdefinierten Scan erstellen möchten, erscheint das Fenster **Scan-Aufgabe**. Hier können Sie die Systembereiche auswählen, die gescannt werden sollen.

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

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

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

1. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.



2. Klicken Sie neben **Scans verwalten** auf **+Scan erstellen**.
3. Geben Sie im Namensfeld einen Namen für den Scan ein, wählen Sie die Bereiche aus, die Sie scannen möchten, und klicken Sie auf **WEITER**.
4. Konfigurieren Sie diese allgemeinen Optionen:
 - ☐ **Nur Anwendungen scannen.** Sie können Bitdefender so einrichten, dass nur aufgerufene Anwendungen gescannt werden.
 - ☐ **Priorität der Scan-Aufgabe.** Sie können festlegen, wie sich ein Scan-Vorgang auf die Systemleistung auswirkt.
 - ☐ **Auto** - Die Priorität des Scanvorgangs hängt von der Systemaktivität ab. Um sicherzustellen, dass der Scanprozess die Systemaktivität nicht beeinträchtigt, entscheidet Bitdefender, ob der Scanprozess mit hoher oder niedriger Priorität ausgeführt werden soll.
 - ☐ **Hoch** - Die Priorität des Scanvorgangs ist hoch. Indem Sie diese Option wählen, erlauben Sie anderen Programmen, langsamer zu laufen, und verkürzen die Zeit, die für den Abschluss des Scanvorgangs benötigt wird.
 - ☐ **Niedrig** - Die Priorität des Scanvorgangs ist niedrig. Wenn Sie diese Option auswählen, können Sie andere Programme schneller ausführen und die Zeit verlängern, die für den Abschluss des Scanvorgangs benötigt wird.
 - ☐ **Aktionen nach dem Scan.** Wählen Sie die Aktion, die von Bitdefender durchgeführt werden soll, wenn keine Bedrohungen gefunden wurden:
 - ☐ Übersichtsfenster anzeigen
 - ☐ Gerät herunterfahren
 - ☐ Schließen Sie das Scan-Fenster
5. Um die Scan-Optionen im Detail zu konfigurieren, klicken Sie auf **Erweiterte Optionen anzeigen**.
Klicken **Nächste**.
6. Sie können bei Bedarf die Option **Scan-Aufgabe planen** aktivieren und dann festlegen, wann der von Ihnen erstellte benutzerdefinierte Scan gestartet werden soll.



- ☐ Beim Systemstart
- ☐ Täglich
- ☐ Monatlich
- ☐ Wöchentlich

Wenn Sie „Täglich“, „Monatlich“ oder „Wöchentlich“ auswählen, ziehen Sie den Schieberegler entlang der Skala, um den gewünschten Zeitraum festzulegen, in dem der geplante Scan beginnen soll.

7. Klicken **Speichern** um die Einstellungen zu speichern und das Konfigurationsfenster zu schließen.

Abhängig von den zu scannenden Orten kann der Scan eine Weile dauern. Wenn während des Scanvorgangs Bedrohungen gefunden werden, werden Sie aufgefordert, die Aktionen auszuwählen, die für die erkannten Dateien durchgeführt werden sollen.

Bei Bedarf können Sie einen bereits durchgeführten benutzerdefinierten Scan einfach erneut ausführen, indem Sie auf den entsprechenden Eintrag in der Liste klicken.

4.3.5. Wie kann ich einen Ordner vom Scan ausnehmen?

Mit Bitdefender können Sie bestimmte Dateien, Ordner oder Dateieindungen vom Scan ausnehmen.

Ausnahmen sollten nur von Benutzern genutzt 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 können Sie einen Ordner Ausschlussliste hinzufügen:

1. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Klicken Sie auf den Reiter **Einstellungen**.



4. Klicken Sie auf **Ausnahmen verwalten**.
5. Klicken **+Fügen Sie eine Ausnahme hinzu**.
6. Geben Sie den Pfad des Ordners, den Sie vom Scannen ausnehmen möchten, in das entsprechende Feld ein.
Alternativ können Sie zu dem Ordner navigieren, indem Sie auf die Schaltfläche „Durchsuchen“ auf der rechten Seite der Benutzeroberfläche klicken, ihn auswählen und auf klicken **OK**.
7. Aktivieren Sie den Schalter neben der Schutzfunktion, die den Ordner nicht scannen soll. Es gibt drei Optionen:
 - ☐ Virenschutz
 - ☐ Abwehr von Online-Bedrohungen
 - ☐ Erweiterte Bedrohungsabwehr
8. Klicken **Speichern** um die Änderungen zu speichern und das Fenster zu schließen.

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

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

1. Deaktivieren Sie den Bitdefender-Echtzeit-Virenschutz:
 - a. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
 - b. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
 - c. Deaktivieren Sie im Fenster **Erweitert** die Option **Bitdefender-Schild**.
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. Verborgene Objekte in Windows anzeigen. Eine Anleitung hierzu finden Sie unter [Wie kann ich in Windows versteckte Objekte anzeigen? \(Seite 91\)](#).
3. Stellen Sie die Datei aus der Quarantäne wieder her:
 - a. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
 - b. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
 - c. Klicken Sie im Fenster **Einstellungen** auf **Quarantäne verwalten**.
 - d. Wählen Sie die Datei aus und klicken Sie auf **Wiederherstellen**.
4. Fügen Sie die Datei zur Ausnahmeliste hinzu. Eine Anleitung hierzu finden Sie unter [Wie kann ich einen Ordner vom Scan ausnehmen? \(Seite 83\)](#).
Standardmäßig fügt Bitdefender wiederhergestellte Dateien automatisch zur Ausnahmeliste hinzu.
5. Aktivieren Sie den Bitdefender-Echtzeit-Virenschutz.
6. Setzen Sie sich mit unserem Support in Verbindung, damit wir die Erkennung beim Update der Bedrohungsinformationen entfernen können. Eine Anleitung hierzu finden Sie unter [Hier wird Ihnen geholfen \(Seite 116\)](#).

4.3.7. 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.

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

So überprüfen Sie ein Scan-Protokoll oder eine erkannte Infektion zu einem späteren Zeitpunkt:



1. Klicken **Benachrichtigungen** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Im **Alle** Wählen Sie auf der Registerkarte die Benachrichtigung über den letzten Scan aus.
Hier finden Sie alle Bedrohungsscan-Ereignisse, einschließlich Bedrohungen, die durch On-Access-Scans, benutzerinitiierte Scans und Statusänderungen für automatische Scans erkannt wurden.
3. In der Benachrichtigungsliste können Sie überprüfen, welche Scans kürzlich durchgeführt wurden. Klicken Sie auf eine Benachrichtigung, um Details dazu anzuzeigen.
4. Um ein Scan-Protokoll zu öffnen, klicken Sie auf **Protokoll anzeigen**.

4.4. Nützliche Informationen

4.4.1. 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. Wechseln Sie zum 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 [Hier wird Ihnen geholfen \(Seite 116\)](#) beschrieben an Bitdefender zu wenden.



4.4.2. Wie kann ich Bitdefender deinstallieren?

So können Sie Ihr Bitdefender Antivirus Free entfernen:

○ In **Windows 7**:

1. Klicken **Start**, gehe zu **Schalttafel** und doppelklicken **Programme und Funktionen**.
2. Finden **Bitdefender Antivirus Free** und auswählen **Deinstallieren**.
3. Klicken Sie im angezeigten Fenster auf **Entfernen**.
4. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

○ In **Windows 8** Und **Windows 8.1**:

1. Suchen Sie auf dem Windows-Startbildschirm **Schalttafel** (z. B. können Sie „Systemsteuerung“ direkt auf dem Startbildschirm eingeben) und dann auf das entsprechende Symbol klicken.
2. Klicken **Ein Programm deinstallieren** oder **Programme und Funktionen**.
3. Finden **Bitdefender Antivirus Free** und auswählen **Deinstallieren**.
4. Klicken **ENTFERNEN** im erscheinenden Fenster.
5. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

○ In **Windows 10** Und **Windows 11**:

1. Klicken Sie auf **Start** und danach auf **Einstellungen**.
2. Drücke den **System** Symbol im Bereich **Einstellungen** und wählen Sie dann aus **Anwendungen**.
3. Finden **Bitdefender Antivirus Free** und auswählen **Deinstallieren**.
4. Klicken **Deinstallieren** erneut, um Ihre Auswahl zu bestätigen.
5. Klicken **ENTFERNEN** im erscheinenden Fenster.
6. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.



Notiz

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

4.4.3. Wie fahre ich das Gerät 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 fertig und möchten ins Bett gehen. Sie möchten aber nun noch Ihr System durch Bitdefender auf Bedrohungen prüfen lassen.

Gehen Sie folgt vor, um das Gerät herunterzufahren, sobald ein Quick-Scan oder System-Scan beendet wurde:

1. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Klicken Sie im Fenster **Scans** neben Quick Scan oder System-Scan auf ... und wählen Sie **Bearbeiten**.
4. Richten Sie den Scan entsprechend Ihrer Anforderungen ein und klicken Sie auf **Weiter**.
5. Markieren Sie das Kästchen neben **Legen Sie fest, für wann Sie diese Aufgabe planen möchten**, und legen Sie fest, wann die Aufgabe beginnen soll.
Wenn Sie „Täglich“, „Monatlich“ oder „Wöchentlich“ auswählen, ziehen Sie den Schieberegler entlang der Skala, um den gewünschten Zeitraum festzulegen, in dem der geplante Scan beginnen soll.
6. Klicken **Speichern**.

Gehen Sie wie folgt vor, um das Gerät nach Abschluss eines benutzerdefinierten Scans herunterzufahren:



1. Klicken Sie neben dem von Ihnen erstellten benutzerdefinierten Scan auf
2. Klicken Sie auf **Weiter** und dann erneut auf **Weiter**.
3. Markieren Sie das Kästchen neben **Legen Sie fest, für wann Sie diese Aufgabe planen möchten** und legen Sie fest, wann die Aufgabe beginnen soll.
4. Klicken **Speichern**.

Wenn keine Bedrohungen gefunden wurden, wird das Gerät 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 \(Seite 58\)](#).

4.4.4. Wie konfiguriere ich Bitdefender für die Verwendung einer Proxy-Internetverbindung?

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



Wichtig

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

So können Sie Ihre Proxy-Einstellungen verwalten:

1. Klicken **Einstellungen** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Wähle aus **Fortschrittlich** Tab.
3. Aktivieren Sie **Proxy-Server**.
4. Klicken Sie auf **Proxy-Änderung**.
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. Sollten der Proxy-Server einen Benutzernamen und ein Passwort erfordern, müssen Sie diese in den entsprechenden Feldern angeben.

Notiz

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.
- **Benutzername** - geben Sie einen für den Proxy-Server gültigen Benutzernamen ein.
- **Passwort** - geben Sie das Passwort des zuvor angegebenen Benutzers 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.

4.4.5. 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. Suchen Sie im **Startmenü** nach **Computer**.



3. Klicken Sie mit der rechten Maustaste auf **Computer** und wählen Sie **Eigenschaften**.
 4. Unter **System** können Sie die Systeminformationen einsehen.
- Unter **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.
Suchen Sie unter **Windows 8.1** nach **Dieser PC**.
 2. Wählen Sie im Menü unten **Eigenschaften**.
 3. Im Bereich System finden Sie Ihren Systemtyp.
- In **Windows 10** Und **Windows 11**:
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.

4.4.6. 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 rufen Sie die **Systemsteuerung** auf.
Unter **Windows 8** und **Windows 8.1**: Suchen Sie im Windows-Startmenü die **Systemsteuerung** (z. B. durch die Eingabe von "Systemsteuerung") und klicken Sie dann auf das entsprechende Symbol.
2. Wählen Sie **Ordneroptionen**.
3. Wechseln Sie zum 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** Und **Windows 11**:

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. Klar **Erweiterungen für bekannte Dateitypen verbergen**.
4. Klar **Geschützte Betriebssystemdateien ausblenden**.
5. Klicken **Anwenden**, dann klick **OK**.

4.4.7. 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 Gerät verwenden, wird dadurch das System instabil. Das Bitdefender Antivirus Free-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 **Start**, gehe zu **Schalttafel** und doppelklicken **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 der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

○ In **Windows 8** Und **Windows 8.1**:



1. Suchen Sie auf dem Windows-Startbildschirm **Schalttafel** (z. B. können Sie „Systemsteuerung“ direkt auf dem Startbildschirm eingeben) und dann auf das entsprechende Symbol klicken.
 2. Klicken **Ein Programm deinstallieren** oder **Programme und Funktionen**.
 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 es aus **Deinstallieren**.
 5. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.
- In **Windows 10** Und **Windows11**:
1. Klicken **Start**, und klicken Sie dann auf Einstellungen.
 2. Drücke den **System** Symbol im Bereich Einstellungen und wählen Sie dann aus **Anwendungen**.
 3. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie es aus **Deinstallieren**.
 4. Klicken **Deinstallieren** erneut, um Ihre Auswahl zu bestätigen.
 5. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann 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.

4.4.8. 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 das Gerät 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**, wenn Sie Zugang zum Internet haben möchten.
4. Drücken Sie die **Eingabetaste** und warten Sie, während Windows im abgesicherten Modus startet.
5. Der Vorgang endet mit einer Bestätigungsmeldung. Klicken Sie zur Bestätigung auf **OK**.
6. Um Windows normal zu starten, starten Sie einfach Ihr System neu.

○ Unter **Windows 8, Windows 8.1, Windows 10 und Windows 11**:

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 Dialogfeld hinter **Öffnen:** ein und klicken Sie dann auf **OK**.
3. Wechseln Sie zum Reiter **Start**.
4. Aktivieren Sie im Bereich **Startoptionen** das Kontrollkästchen **Abgesicherter Start**.
5. Klicken Sie auf **Netzwerk** und danach 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 wieder zurück, um Ihr System im normalen Modus neu zu starten. Kehren Sie dazu zur **Systemkonfiguration** zurück und deaktivieren Sie das Kästchen **Abgesicherter Start**. Klicken Sie auf



OK und danach auf **Neustart**. Warten Sie, bis die neuen Einstellungen übernommen werden.



5. PROBLEMLÖSUNG

5.1. Verbreitete Probleme beheben

Dieses Kapitel zeigt einige Probleme bei der Benutzung von BitDefender auf und bietet mögliche Lösungen dazu. Die meisten dieser Probleme können durch die geeigneten Einstellungen im Produkt behoben werden.

- [Mein System scheint langsamer zu sein \(Seite 96\)](#)
- [Der Scan startet nicht \(Seite 98\)](#)
- [Ich kann eine App nicht mehr verwenden \(Seite 100\)](#)
- [Was können Sie tun, wenn Bitdefender eigentlich sichere Websites, Domains, IP-Adressen oder Online-Anwendungen blockiert? \(Seite 101\)](#)
- [Wie man Bitdefender-Updates auch mit einer langsamen Internet-Verbindung durchführen kann \(Seite 102\)](#)
- [Bitdefender-Dienste antworten nicht \(Seite 103\)](#)
- [Der Spam-Schutz-Filter funktioniert nicht richtig](#)
- [Das automatische Einfügen funktioniert bei meiner Geldbörse nicht](#)
- [Entfernen von Bitdefender fehlgeschlagen \(Seite 104\)](#)
- [Mein System fährt nach der Installation von Bitdefender nicht mehr hoch \(Seite 105\)](#)

Wenn Sie Ihr Problem hier nicht finden oder dieser weiterhin besteht, können Sie kontakt zu unserem BitDefender Technischen Support aufnehmen, wie beschrieben in {1}{2}.

5.1.1. Mein System scheint langsamer zu sein

Nach der Installation einer Sicherheitssoftware ist eine geringfügige Verlangsamung des Systems bis zu einem gewissen Grad normal.

Wenn Sie eine erhebliche Systemverlangsamung feststellen, kann dies folgende Ursachen haben:

- **Bitdefender ist nicht die einzige auf Ihrem System installierte Sicherheits-Software.**
Obwohl Bitdefender bereits auf Ihrem System installierte Sicherheitsprogramme während der Installation sucht und entfernt,



empfehlen wir dennoch, jede andere Sicherheitslösung von Ihrem Rechner zu entfernen, bevor Sie die Installation von Bitdefender starten. Weitere Informationen finden Sie im Kapitel [Wie entferne ich andere Sicherheitslösungen? \(Seite 92\)](#).

○ **Die Systemvoraussetzungen für die Ausführung von Bitdefender sind nicht erfüllt.**

Wenn Ihr Gerät die Systemvoraussetzungen nicht erfüllt, verlangsamt dies Ihr System, insbesondere dann, wenn mehrere Anwendungen gleichzeitig laufen. Weitere Informationen finden Sie im Kapitel [Systemanforderungen \(Seite 4\)](#).

○ **Sie haben Apps installiert, die Sie nicht verwenden.**

Auf jedem Gerät sind Programme oder Anwendungen installiert, 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 Geräteleistung aus. Stellen Sie sicher, dass Ihr System regelmäßig gescannt wird, mindestens einmal pro Woche. Wir empfehlen, 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 **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Klicken Sie im Fenster **Scans** neben **System-Scan** auf die Schaltfläche **Scan starten**.
4. Befolgen Sie die Anweisungen des Assistenten.



5.1.2. Der Scan startet nicht

Dieses Problem kann folgende Ursachen haben:

- Eine vorherige Installation von Bitdefender wurde nicht vollständig entfernt oder es handelt sich um eine fehlerhafte Bitdefender-Installation.

Installieren Sie Bitdefender in diesem Fall neu:

- In **Windows 7**:
 1. Klicken **Start**, gehe zu **Schalttafel** und doppelklicken **Programme und Funktionen**.
 2. Finden **Bitdefender Antivirus Free** und auswählen **Deinstallieren**.
 3. Klicken **NEU INSTALLIEREN** im erscheinenden Fenster.
 4. Warten Sie, bis die Neuinstallation abgeschlossen ist und starten Sie Ihr System neu.
- In **Windows 8** Und **Windows 8.1**:
 1. Suchen Sie auf dem Windows-Startbildschirm **Schalttafel** (z. B. können Sie „Systemsteuerung“ direkt auf dem Startbildschirm eingeben) und dann auf das entsprechende Symbol klicken.
 2. Klicken **Deinstallieren** ein Programm bzw **Programme und Funktionen**.
 3. Finden **Bitdefender Antivirus Free** und auswählen **Deinstallieren**.
 4. Klicken **NEU INSTALLIEREN** im erscheinenden Fenster.
 5. Warten Sie, bis der Neuinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.
- In **Windows 10** Und **Windows 11**:
 1. Klicken **Start**, dann klick **Einstellungen**.
 2. Drücke den **System** Symbol im Bereich Einstellungen und wählen Sie dann aus **Installierte Anwendungen**.
 3. Finden **Bitdefender Antivirus Free** und auswählen **Deinstallieren**.
 4. Klicken **Deinstallieren** erneut, um Ihre Auswahl zu bestätigen.
 5. Klicken **NEU INSTALLIEREN** im erscheinenden Fenster.



6. Warten Sie, bis der Neuinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.



Notiz

Durch Befolgen dieses Neuinstallationsverfahrens werden benutzerdefinierte Einstellungen gespeichert und stehen im neu installierten Produkt zur Verfügung. Andere Einstellungen können auf ihre Standardkonfiguration zurückgesetzt werden.

○ **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?](#) (Seite 92).
2. Bitdefender erneut installieren:

○ In **Windows 7**:

- a. Klicken **Start**, gehe zu **Schalttafel** und doppelklicken **Programme und Funktionen**.
- b. Finden **Bitdefender Antivirus Free** und auswählen **Deinstallieren**.
- c. Klicken **NEU INSTALLIEREN** im erscheinenden Fenster.
- d. Warten Sie, bis der Neuinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

○ In **Windows 8** Und **Windows 8.1**:

- a. Suchen Sie auf dem Windows-Startbildschirm **Schalttafel** (z. B. können Sie „Systemsteuerung“ direkt auf dem Startbildschirm eingeben) und dann auf das entsprechende Symbol klicken.
- b. Klicken **Deinstallieren** ein Programm bzw **Programme und Funktionen**.
- c. Finden **Bitdefender Antivirus Free** und auswählen **Deinstallieren**.
- d. Klicken **NEU INSTALLIEREN** im erscheinenden Fenster.



- e. Warten Sie, bis der Neuinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

○ In **Windows 10** Und **Windows 11**:

- a. Klicken **Start**, dann klick **Einstellungen**.
- b. Drücke den **System** Symbol im Bereich Einstellungen und wählen Sie dann aus **Installierte Anwendungen**.
- c. Finden **Bitdefender Antivirus Free** und auswählen **Deinstallieren**.
- d. Klicken **Deinstallieren** erneut, um Ihre Auswahl zu bestätigen.
- e. Klicken Sie im angezeigten Fenster auf **NEU INSTALLIEREN**
- f. Warten Sie, bis der Neuinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

 Notiz

Durch Befolgen dieses Neuinstallationsverfahrens werden benutzerdefinierte Einstellungen gespeichert und stehen im neu installierten Produkt zur Verfügung. Andere Einstellungen können auf ihre Standardkonfiguration zurückgesetzt werden.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den BitDefender Support wie in folgendem Abschnitt beschrieben: [Hier wird Ihnen geholfen \(Seite 116\)](#).

5.1.3. Ich kann eine App nicht mehr verwenden

Dieses Problem tritt auf, wenn Sie versuchen, ein Programm zu verwenden, das vor der Installation von Bitdefender einwandfrei funktioniert hatte.

Nach der Installation von Bitdefender könnten folgende Situationen eintreten:

- Sie könnten 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 ausnehmen.

So können Sie das Programm zur Ausnahmeliste hinzufügen:

1. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Im **ERWEITERTE BEDROHUNGSABWEHR** Bereich, klicken Sie auf **Offen**.
3. Im **Einstellungen** Fenster, klicken **Ausnahmen verwalten**.
4. Klicken **+Fügen Sie eine Ausnahme hinzu**.
5. Geben Sie den Pfad der ausführbaren Datei, die Sie vom Scan ausnehmen möchten, in das entsprechende Feld ein.
Alternativ können Sie zur ausführbaren Datei navigieren, indem Sie auf die Schaltfläche „Durchsuchen“ auf der rechten Seite der Benutzeroberfläche klicken, sie auswählen und auf klicken **OK**.
6. Schalten Sie den Schalter daneben ein **Erweiterte Bedrohungsabwehr**.
7. Klicken **Speichern**.

Wenn diese Informationen nicht hilfreich waren, können Sie sich wie im Abschnitt beschrieben an Bitdefender wenden, um Support zu erhalten [Hier wird Ihnen geholfen \(Seite 116\)](#).

5.1.4. Was können Sie tun, wenn Bitdefender eigentlich sichere Websites, Domains, IP-Adressen oder Online-Anwendungen blockiert?

Bitdefender ermöglicht Ihnen sicheres Surfen im Netz, indem es Ihren Internet-Datenverkehr filtert und schädliche Inhalte blockiert. Es kann jedoch vorkommen, dass Bitdefender eigentlich sichere Websites, Domains, IP-Adressen oder Online-Anwendungen als unsicher einstuft, wodurch diese dann durch den Bitdefender-Scan des HTTP-Datenverkehrs irrtümlich blockiert werden.

Sollte die gleiche Seite, Domain, IP-Adresse oder Online-Anwendung wiederholt blockiert werden, können Sie diese zu den Ausnahmen



hinzufügen, damit sie von den Bitdefender-Engines nicht mehr gescannt werden. So können Sie ungestört im Internet surfen.

So können Sie eine Website zu den **Ausnahmen** hinzufügen:

1. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Im **VORBEUGUNG VON ONLINE-BEDROHUNGEN** Bereich, klicken Sie auf **Einstellungen**.
3. Klicken **Ausnahmen verwalten**.
4. Klicken **+Fügen Sie eine Ausnahme hinzu**.
5. Geben Sie in das entsprechende Feld den Namen der Website, den Namen der Domain oder die IP-Adresse ein, die Sie zu Ausnahmen hinzufügen möchten.
6. Klicken Sie auf den Schalter neben **Abwehr von Online-Bedrohungen**.
7. Klicken **Speichern** um die Änderungen zu speichern und das Fenster zu schließen.

Nur Websites, Domains, IP-Adressen und Anwendungen, denen Sie uneingeschränkt vertrauen, sollten dieser Liste hinzugefügt werden. Diese werden dann von den folgenden Engines vom Scan ausgenommen: Bedrohung, Phishing und Betrug.

Wenn diese Informationen nicht hilfreich waren, können Sie sich wie im Abschnitt beschrieben an Bitdefender wenden, um Support zu erhalten [Hier wird Ihnen geholfen \(Seite 116\)](#).

5.1.5. 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 **Einstellungen** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
2. Wähle aus **Aktualisieren** Tab.
3. Deaktivieren Sie den Schalter **Update im Hintergrund**.



4. Beim nächsten Update werden Sie aufgefordert, das Update auszuwählen, das Sie herunterladen möchten. Wählen Sie nur **Virensignatur-Update**.
5. Bitdefender wird nur die Datenbank mit den Bedrohungsinformationen herunterladen und installieren.

5.1.6. Bitdefender-Dienste antworten nicht

Dieser Artikel hilft Ihnen bei der Lösung des **BitDefender Dienste antworten nicht** Problems. 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 Dienste.
- einige der BitDefender Dienste sind gestoppt.
- andere Sicherheitslösungen werden gleichzeitig mit Bitdefender auf Ihrem Gerät ausgeführt.

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 das Gerät 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 Geräts wird das Problem üblicherweise behoben.
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? \(Seite 92\)](#).



Sollte der Fehler weiterhin auftreten, wenden Sie sich bitte an unsere Support-Mitarbeiter, wie in Abschnitt [Hier wird Ihnen geholfen \(Seite 116\)](#) beschrieben.

5.1.7. Entfernen von Bitdefender 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 **Start**, gehe zu **Schalttafel** und doppelklicken **Programme und Funktionen**.
2. Finden **Bitdefender Antivirus Free** und auswählen **Deinstallieren**.
3. Klicken **ENTFERNEN** im erscheinenden Fenster.
4. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

○ In **Windows 8** Und **Windows 8.1**:

1. Suchen Sie auf dem Windows-Startbildschirm **Schalttafel** (z. B. können Sie „Systemsteuerung“ direkt auf dem Startbildschirm eingeben) und dann auf das entsprechende Symbol klicken.
2. Klicken **Ein Programm deinstallieren** oder **Programme und Funktionen**.
3. Finden **Bitdefender Antivirus Free** und auswählen **Deinstallieren**.
4. Klicken **ENTFERNEN** im erscheinenden Fenster.
5. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

○ In **Windows 10** Und **Windows11**:



1. Klicken **Start**, und klicken Sie dann auf Einstellungen.
2. Drücke den **System** Symbol im Bereich Einstellungen und wählen Sie dann aus **Installierte Anwendungen**.
3. Finden **Bitdefender Antivirus Free** und auswählen **Deinstallieren**.
4. Klicken **Deinstallieren** erneut, um Ihre Auswahl zu bestätigen.
5. Klicken **ENTFERNEN** im erscheinenden Fenster.
6. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

5.1.8. 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 installiert 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 unter [Wie führe ich einen Neustart im abgesicherten Modus durch? \(Seite 93\)](#).
2. Entfernen Sie Bitdefender von Ihrem System:

○ In Windows 7:

- a. Klicken **Start**, gehe zu **Schalttafel** und doppelklicken **Programme und Funktionen**.
- b. Finden **Bitdefender Antivirus Free** und auswählen **Deinstallieren**.



- c. Klicken **ENTFERNEN** im erscheinenden Fenster.
- d. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.
- e. Starten Sie Ihren Computer im Normalmodus neu.

○ In **Windows 8 Und Windows 8.1:**

- a. Suchen Sie auf dem Windows-Startbildschirm **Schalttafel** (z. B. können Sie „Systemsteuerung“ direkt auf dem Startbildschirm eingeben) und dann auf das entsprechende Symbol klicken.
- b. Klicken **Ein Programm deinstallieren** oder **Programme und Funktionen**.
- c. Finden **Bitdefender Antivirus Free** und auswählen **Deinstallieren**.
- d. Klicken **ENTFERNEN** im erscheinenden Fenster.
- e. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.
- f. Starten Sie Ihr System im normalen Modus neu.

○ In **Windows 10 Und Windows11:**

- a. Klicken **Start**, und klicken Sie dann auf Einstellungen.
- b. Drücke den **System** Symbol im Bereich Einstellungen und wählen Sie dann aus **Installierte Anwendungen**.
- c. Finden **Bitdefender Antivirus Free** und auswählen **Deinstallieren**.
- d. Klicken **Deinstallieren** erneut, um Ihre Auswahl zu bestätigen.
- e. Klicken **ENTFERNEN** im erscheinenden Fenster.
- f. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.
- g. Starten Sie Ihr System im normalen Modus neu.

3. Installieren Sie Ihr Bitdefender-Produkt neu.



- Sie hatten zuvor eine andere Sicherheitslösung im Einsatz und haben diese nicht vollständig entfernt.

Um dies zu lösen:

1. Starten Sie Ihr System neu und wechseln Sie in den abgesicherten Modus. Wie das geht, erfahren Sie unter [Wie führe ich einen Neustart im abgesicherten Modus durch? \(Seite 93\)](#).
2. Entfernen Sie die andere Sicherheitslösung von Ihrem System:

- In **Windows 7**:

- a. Klicken **Start**, gehe zu **Schalttafel** und doppelklicken **Programme und Funktionen**.
- b. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.
- c. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

- In **Windows 8** Und **Windows 8.1**:

- a. Suchen Sie auf dem Windows-Startbildschirm **Schalttafel** (z. B. können Sie „Systemsteuerung“ direkt auf dem Startbildschirm eingeben) und dann auf das entsprechende Symbol klicken.
- b. Klicken **Ein Programm deinstallieren** oder **Programme und Funktionen**.
- c. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie es aus **Entfernen**.
- d. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

- In **Windows 10** Und **Windows 11**:

- a. Klicken **Start**, und klicken Sie dann auf **Einstellungen**.
- b. Drücke den **System** Symbol im Bereich **Einstellungen** und wählen Sie dann aus **Installierte Anwendungen**.
- c. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie es aus **Deinstallieren**.



- d. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann 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.

Um dies zu lösen:

1. Starten Sie Ihr System neu und wechseln Sie in den abgesicherten Modus. Wie das geht, erfahren Sie unter [Wie führe ich einen Neustart im abgesicherten Modus durch? \(Seite 93\)](#).
2. Nutzen Sie die Systemwiederherstellung von Windows, um das Gerät 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 [Hier wird Ihnen geholfen \(Seite 116\)](#) beschrieben.

5.2. Entfernung von Bedrohungen

Bedrohungen können Ihr System auf vielfältige Art und Weise beeinträchtigen. Wie Bitdefender auf diese Malware darauf reagiert, hängt von der Art der Bedrohung ab. Da Bedrohungen ihr Verhalten ständig ändern, ist es schwierig ein Muster für ihr Verhalten und ihre Aktionen festzulegen.

Es gibt Situationen, in denen Bitdefender eine Bedrohung Ihres Systems nicht automatisch entfernen kann. In solch einem Fall ist Ihre Intervention nötig.

- [Rettungsumgebung](#)
- [Was ist zu tun, wenn Bitdefender Bedrohungen auf Ihrem Gerät findet? \(Seite 109\)](#)



- Wie entferne ich eine Bedrohung aus einem Archiv? (Seite 110)
- Wie entferne ich eine Bedrohung aus einem E-Mail-Archiv? (Seite 112)
- Wie gehe ich vor, wenn ich eine Datei für gefährlich halte? (Seite 113)
- Wobei handelt es sich bei den passwortgeschützten Dateien im Scan-Protokoll? (Seite 113)
- Wobei handelt es sich bei den übersprungenen Objekten im Scan-Protokoll? (Seite 114)
- Wobei handelt es sich bei den zu stark komprimierten Dateien im Scan-Protokoll? (Seite 114)
- Warum hat Bitdefender eine infizierte Datei automatisch gelöscht? (Seite 114)

Wenn Sie Ihr Problem hier nicht finden können oder die vorgestellten Lösungen es nicht lösen, können Sie sich wie in Kapitel beschrieben an die Vertreter des technischen Supports von Bitdefender wenden [Hier wird Ihnen geholfen](#) (Seite 116).

5.2.1. Was ist zu tun, wenn Bitdefender Bedrohungen auf Ihrem Gerät findet?

Es gibt verschiedene Möglichkeiten, wie Sie von einer Bedrohung auf Ihrem Gerät erfahren:

- Sie haben einen Scan Ihres Geräts durchgeführt und Bitdefender hat infizierte Objekte gefunden.
- Eine Bedrohungswarnung informiert Sie, dass Bitdefender einen oder mehrere Bedrohungen auf Ihrem Gerät blockiert 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 Echtzeit-Virenschutz von Bitdefender:
 - a. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
 - b. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
 - c. Im **Fortschrittlich** Fenster, ausschalten **Bitdefender-Schild**.
2. Zeigen Sie versteckte Objekte in Windows an. Wie das geht, erfahren Sie unter [Wie kann ich in Windows versteckte Objekte anzeigen? \(Seite 91\)](#).
3. Blättern Sie zum Laufwerk, in dem die infizierte Datei gespeichert ist (siehe Scan-Protokoll) und löschen Sie sie.
4. Schalten Sie den Echtzeit-Virenschutz von Bitdefender ein.

Falls die Infektion mit der ersten Methode nicht entfernt werden konnte:

1. Starten Sie Ihr System neu und wechseln Sie in den abgesicherten Modus. Wie das geht, erfahren Sie unter [Wie führe ich einen Neustart im abgesicherten Modus durch? \(Seite 93\)](#).
2. Zeigen Sie versteckte Objekte in Windows an. Wie das geht, erfahren Sie unter [Wie kann ich in Windows versteckte Objekte anzeigen? \(Seite 91\)](#).
3. Navigieren Sie zum Speicherort der infizierten Datei (überprüfen Sie das Scan-Protokoll) und löschen Sie sie.
4. Starten Sie Ihren Computer neu und starten Sie den Normalmodus.

Wenn diese Informationen nicht hilfreich waren, können Sie sich wie im Abschnitt beschrieben an Bitdefender wenden, um Support zu erhalten [Hier wird Ihnen geholfen \(Seite 116\)](#).

5.2.2. 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 Echtzeit-Virenschutz von Bitdefender:
 - a. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
 - b. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
 - c. Im **Fortschrittlich** Fenster, ausschalten **Bitdefender-Schild**.
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.



Notiz

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 diese Informationen nicht hilfreich waren, können Sie sich wie im Abschnitt beschrieben an Bitdefender wenden, um Support zu erhalten [Hier wird Ihnen geholfen \(Seite 116\)](#).

5.2.3. 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 Echtzeit-Virenschutz von Bitdefender:
 - a. Klicken **Schutz** im Navigationsmenü auf der [Bitdefender-Oberfläche](#).
 - b. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
 - c. Im **Fortschrittlich** Fenster, ausschalten **Bitdefender-Schild**.
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". Markieren Sie die persönlichen Ordner (.pst), die 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 (.pst), die Sie komprimieren wollen, und klicken Sie auf "Einstellungen". Klicken Sie auf "Jetzt komprimieren".

6. Schalten Sie den Echtzeit-Virenschutz von Bitdefender ein.

Wenn diese Informationen nicht hilfreich waren, können Sie sich wie im Abschnitt beschrieben an Bitdefender wenden, um Support zu erhalten [Hier wird Ihnen geholfen \(Seite 116\)](#).

5.2.4. 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 unter [How do I scan my system?](#) .
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 unter [Hier wird Ihnen geholfen \(Seite 116\)](#).

5.2.5. 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 Geräts 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.

5.2.6. 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.

5.2.7. 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.

5.2.8. 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.

Bei bestimmten Arten von Bedrohungen ist eine Desinfektion nicht möglich, da die erkannte Datei vollständig bösartig ist. In solchen 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.



6. HILFE UND SUPPORT

6.1. Hier wird Ihnen geholfen

Bitdefender bietet seinen Kunden einen konkurrenzlos schnellen und kompetenten Support. Wenn Sie ein Problem oder eine Frage zu Ihrem Bitdefender-Produkt haben, können Sie verschiedene Online-Ressourcen nutzen, um eine Lösung bzw. eine Antwort zu finden. Darüber hinaus können Sie sich jederzeit an den Bitdefender-Kundendienst wenden. Unsere Support-Mitarbeiter werden Ihre Fragen zeitnah beantworten und Ihnen die notwendige Unterstützung bieten.

6.2. Online-Ressourcen

Bei Problemen und Fragen in Zusammenhang mit Bitdefender stehen verschiedene Online-Ressourcen zur Verfügung.

- Bitdefender-Support-Center:
<https://www.bitdefender.de/consumer/support/>
- Die Bitdefender Expert Community:
<https://community.bitdefender.com/de>
- Bitdefender Cyberpedia:
<https://www.bitdefender.com/cyberpedia/>

Weitere Informationen über Computersicherheit, Bitdefender-Produkte und unsere Firma finden Sie über Ihre Liebessuchmaschine.

6.2.1. 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.

Die Bitdefender Support Center ist zudem öffentlich zugänglich und komplett durchsuchbar. Durch diese Art der Informationsbereitstellung bieten wir unseren Kunden eine weitere Möglichkeit, technische



Grundlagen und Fachwissen über unsere Produkte zu erlangen. 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 ist jederzeit unter der folgenden Adresse erreichbar: <https://www.bitdefender.de/consumer/support/>.

6.2.2. Die Bitdefender Experten Community

Die Experten-Community ist eine Plattform, auf der sich Bitdefender-Experten, -Anwender und -Fans einbringen, Ideen austauschen, sich gegenseitig unterstützen und ihr Wissen und ihre Lösungen mit anderen teilen. Hier werden zudem viele Ideen geboren und unsere Entwickler finden wichtiges Feedback. Unsere Community-Mitglieder sind erfahrene Bitdefender-Anwender, die Freude daran haben, anderen zu helfen. Dank ihres unschätzbaren Beitrags und ihres freiwilligen Engagements konnten wir eine Wissensdatenbank schaffen, in der Anwender nützliche Antworten und Anleitungen finden können, aber auch das Zwischenmenschliche seinen Platz hat.

Hier können Sie in einen echten Austausch mit Menschen treten, die Bitdefender selbst auf ihren Geräten nutzen. Die Community verbindet Sie mit unseren Mitgliedern und verschafft Ihrer Stimme Gehör. Hier werden Sie sich gerne einbringen, weil Sie wissen, dass Ihre Meinung und Ihr Beitrag respektiert und geschätzt werden. Als Anbieter Ihrer Wahl sind wir stets bestrebt, Ihnen beispiellos schnellen und kompetenten Support zu bieten und möchten Sie an unserer Seite wissen. Darum haben wir diese Community geschaffen.

Hier geht's zur Website unserer Expert Community:

<https://community.bitdefender.com/de>

6.2.3. Bitdefender Cyberpedia

In der Bitdefender Cyberpedia finden Sie alles Wissenswerte zu den neuesten Cyberbedrohungen. Hier teilen Bitdefender-Experten Tipps und Tricks, wie Sie sich vor Hackern, Datenpannen, Identitätsdiebstahl und Identitätsbetrug in den sozialen Medien schützen können.

Die Bitdefender Cyberpedia finden Sie hier:

<https://www.bitdefender.com/cyberpedia>.



6.3. Kontaktinformation

Effiziente und kundenorientierte Kommunikation ist der Schlüssel zu einem erfolgreichen Geschäftsmodell. Bereits seit 2001 setzt BITDEFENDER alles daran, die bereits hochgesteckten Erwartungen unserer Kunden und Partner immer wieder zu übertreffen und diese Tradition wollen wir auch in Zukunft fortführen. Für jedwede Fragen stehen wir Ihnen deshalb gerne zur Verfügung. Kontaktieren Sie uns dazu einfach über unser **Bitdefender Support Center**.

<https://www.bitdefender.de/consumer/support/>

6.3.1. Lokale Vertriebspartner

Die Bitdefender Händler stehen für Fragen und Informationen in ihren jeweiligen Regionen jederzeit zur Verfügung, sowohl für vertriebliche als auch für allgemeine Anfragen.

So finden Sie einen Bitdefender Distributor in Ihrem Land:

1. Mehr dazu unter <https://www.bitdefender.de/partners/partner-locator.html>.
2. Geben Sie über die entsprechenden Optionen Ihren Wohnort und Ihr Land an.



GLOSSAR

Aktivierungscode

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.

ActiveX

ActiveX ist ein Programmuster, dass von anderen Programmen und Betriebssystemkomponenten unter Windows aufgerufen werden kann. Die ActiveX Technologie wird von Microsofts Internet Explorer benutzt, damit interaktive Webseiten eher wie Programme und nicht wie statische Seiten angezeigt werden. Mit ActiveX können die Benutzer z.B. Fragen stellen oder beantworten, Buttons verwenden, oder verschiedenartige Interaktionen mit der Webseite herstellen. ActiveX-Steuerelemente werden oft in Visual Basic geschrieben. Erwähnenswert ist, dass bei ActiveX die Sicherheitskontrollen fehlen, deshalb raten Computersicherheitsexperten davon ab, ActiveX über das Internet zu nutzen.

Advanced Persistent Threat

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.

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.

Hintertür

Eine Sicherheitslücke eines Systems, die der Entwickler oder Verwalter absichtlich hinterlässt. Der Grund dafür muss nicht immer bösartig sein. Manche Betriebssysteme haben schon bei der Fabrikation privilegierte Konten, damit diese von den Kundendienst-Technikern oder Programmierern der Hersteller benutzt werden können.

Bootsektor

Der erste Sektor einer Festplatte oder Diskette. Hier liegen Daten, die das Betriebssystem zum Booten (Starten) braucht.

Bootvirus

Eine Bedrohung, die 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.



Browser

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.

Brute-Force-Angriff

Ein Angriff mit dem Ziel, sich Zugang zu einem passwortgeschützten System zu verschaffen, bei dem in schneller Abfolge häufige Passwortkombinationen durchprobiert werden.

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.

Cookies

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.



Cybermobbing

Wenn Altersgenossen oder Fremde absichtlich Kinder misshandeln, um sie körperlich zu verletzen. Um emotionale Schäden anzurichten, schicken die Täter verletzende Nachrichten oder unvorteilhafte Fotos, so dass sich ihre Opfer von anderen isolieren oder entmutigt werden.

Wörterbuchangriff

Ein Angriff mit dem Ziel, sich Zugang zu einem passwortgeschützten System zu verschaffen, bei dem alle möglichen Wörter aus einem Wörterbuch als potenzielle Passwörter eingegeben werden. Dieselbe Methode wird auch verwendet um Schlüssel für verschlüsselte Nachrichten oder Dokumente zu erraten. Wörterbuchangriffe funktionieren, weil viele Benutzer kurze, leicht zu erratende Wörter als Passwörter benutzen.

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.

Download

Kopiert Daten (gewöhnlich eine ganze Datei) von einer Hauptquelle auf ein Peripheriegerät. Der Begriff bezeichnet oft den Kopiervorgang von einem Online Service auf den eigenen Rechner. Download oder Herunterladen kann auch das Kopieren einer Datei von einem Netzwerkserver auf einen Netzwerkrechner bedeuten.

E-Mail

Elektronische Post. Ein Dienst, der Nachrichten an andere Rechner über ein lokales oder ein globales Netzwerk übermittelt.

Ereignisse

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.

Exploits



Eine Möglichkeit, Fehler oder Schwachstellen in Computersoftware und -hardware für seine Zwecke auszunutzen. So können Hacker die Kontrolle über Computer oder Netzwerke übernehmen.

Fehlalarme

Erscheint, wenn ein Virens Scanner eine Datei als infiziert erkennt, obwohl dies nicht der Fall ist.

Dateinamenerweiterung

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.

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 auf dem Client laufen, können diese keine Daten auf der Clientmaschine lesen oder schreiben. Zusätzlich sind die Applets weiter begrenzt, so dass sie nur Daten aus der Domäne lesen und beschreiben können, die sie unterstützen.

Keylogger

Ein Keylogger ist eine Anwendung, die alle Ihre Tastenanschläge aufzeichnet. Keylogger sind an sich nicht schädlich. Sie können auch legitim eingesetzt werden, um beispielsweise die Aktivitäten von Angestellten oder Kindern zu überwachen. Sie werden jedoch zunehmend von Cyber-Kriminellen mit bösartiger Absicht eingesetzt (um beispielsweise private Daten wie Benutzernamen oder Passwörter zu sammeln).

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.

Mail-Client

Ein E-Mail-Client ist eine Anwendung, die das Senden und Empfangen von E-Mails ermöglicht.

Arbeitsspeicher

Interne Speicherzonen im Rechner. Der Begriff Arbeitsspeicher bedeutet Datenträger in Form von sehr schnellen Chips. Das Wort Speicher ist der Speicherplatz, der sich auf Magnetbändern oder Datenträgern befindet. Jeder Rechner hat eine gewisse Menge Arbeitsspeicher. Dieser wird auch Hauptspeicher oder RAM genannt.

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.

Online-Missbrauch

Wenn Personen versuchen, Minderjährige oder Jugendliche anzusprechen, um sie in illegale sexuelle Aktivitäten zu verwickeln. Soziale Netzwerke sind der ideale Ort, um verletzlichen Kindern nachzustellen und sie zu sexuellen Aktivitäten zu verführen, sei es online oder persönlich.

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 zum Komprimieren von Dateien würde jedoch die Leerzeichen durch ein spezielles Zeichen der Leerzeichenreihe, gefolgt von der Anzahl der zu ersetzenden Leerzeichen, ersetzen. In diesem Fall würden für die zehn Leerzeichen nur zwei Bytes benötigt. Dies ist nur eine Komprimierungstechnik - es gibt noch viele weitere.

Pfad

Zeigt die Stelle an, an der sich eine Datei auf einem Computer befindet. Diese Pfadangaben enthalten gewöhnlich den hierarchischen Aufbau des Dateiverzeichnisses von oben nach unten.

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.

Polymorphic 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.

Port

Eine Schnittstelle an einem Computer, an die ein Gerät angeschlossen werden kann. PCs haben verschiedene Arten von Anschlüssen. Intern gibt es mehrere Anschlüsse für den Anschluss von Laufwerken, Bildschirmen und Tastaturen. Extern haben PCs Anschlüsse für den Anschluss von Modems, Druckern, Mäusen und anderen Peripheriegeräten.

In TCP/IP und UDP Netzwerken, ein Endpunkt zu logischen Verbindungen. Die Schnittstellennummer gibt die Art der Schnittstelle an. Zum Beispiel, Schnittstelle 80 wird für HTTP Traffic verwendet.

Ransomware

Ransomware ist bösartige Software, die das System des Opfers sperrt und nur gegen ein Lösegeld wieder entfernt wird. CryptoLocker, CryptoWall und TeslaWall sind einige bekanntere Beispiele für Ransomware.

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.

Berichtsdatei

Eine Datei, die stattgefundenen Aktivitäten aufzeichnet. Zum Beispiel speichert BitDefender eine Logdatei mit den geprüften Pfaden, Ordnern und der Archivanzahl, aber auch die geprüften, infizierten oder verdächtigen Dateien.

Rootkit



Ein Rootkit ist eine Sammlung von Software-Tools, die den Zugriff auf ein System auf Administratorebene ermöglichen. Der Begriff wurde erstmals für UNIX-Betriebssysteme verwendet und bezog sich auf neu kompilierte Tools, die Eindringlingen administrative Rechte verschafften und es ihnen ermöglichten, ihre Anwesenheit zu verbergen, um der Erkennung durch den Systemadministrator zu entgehen.

Die Hauptaufgabe von Rootkits besteht darin, Prozesse, Dateien, Logins und Protokolle zu verbergen. Sie können auch Daten von Terminals, Netzwerkverbindungen oder Peripheriegeräten abfangen, wenn sie die entsprechende Software enthalten.

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.

Skript

Ein anderer Begriff für Makro- oder Batchdatei. Ein Skript ist eine Befehlsliste, die ohne Benutzereingriff ausgeführt werden kann.

Spam

Junk-E-Mail oder Junk-Beiträge 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.

Systemstartelemente

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.

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.

Taskleiste

Die Symbolleiste wurde mit Windows 95 eingeführt und befindet sich auf der Windows Taskleiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet). Sie enthält kleine Icons zur Information und zum leichteren Zugriff, zum Beispiel: Fax, Drucker, Modem, Lautstärke und mehr. Um auf die Details und Steuerungen 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.

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.

Update der Bedrohungsinformationen

Das binäre Muster einer Bedrohung, wird von der Sicherheitslösung zur Erkennung und Beseitigung einer Bedrohung genutzt.

Trojaner

Ein bösartiges Programm, das sich als eine legitime Anwendung ausgibt. Anders als Schad-Software und Würmer vervielfältigen sich Trojaner nicht selbst, können aber dennoch großen Schaden anrichten. Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Bedrohungen zu befreien, stattdessen aber den Rechner infiziert.

Der Begriff entstammt einer Geschichte in Homer's "Ilias", in der die Griechen Ihren Feinden, den Trojanern, angeblich als Sühnegabe ein hölzernes Pferd schenkten. Aber, nachdem die Trojaner das Pferd innerhalb der Stadtmauern gebracht hatten, kamen die in dem Bauch des hölzernen Pferdes versteckten Soldaten heraus, öffneten die Tore der Stadt und ermöglichten somit ihren Landsmännern in die Stadt einzudringen und auf diese Weise Troja zu besetzen.

Update

Neue Softwareversionen oder Hardwareprodukte, die eine ältere Version ersetzen. Die Update-Installationsroutine sucht nach älteren Versionen auf dem Rechner, 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.

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 über ein Netzwerk ausbreitet und sich dabei selbst reproduziert. Es kann sich nicht an andere Programme anhängen.