Bitdefender®
ANTIVIRUS FOR MAC

BENUTZERHAN DBUCH

Mac

Bitdefender Antivirus for Mac

Bedienungsanleitung

Veröffentlichungsdatum: 24.11.2022
Copyright © 2022 Bitdefender

Impressum

Alle Rechte vorbehalten. Kein Teil dieses Buches darf ohne schriftliche Genehmigung eines autorisierten Vertreters von Bitdefender in irgendeiner Form oder mit irgendwelchen Mitteln, 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 keinerlei 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

Zielsetzung und Zielgruppe

Dieses Benutzerhandbuch ist für alle Macintosh-Benutzer vorgesehen, die sich für Bitdefender Antivirus for Mac als Sicherheitslösung für Ihre Computer entschieden haben. Die in diesem Dokument beschriebenen Informationen sind nicht nur für IT-Profis gedacht, sondern auch für all diejenigen die sich nur in Ihrer Freizeit mit dem Computer beschäftigen.

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

Viel Spaß mit diesen nützlichen und informativen Handbuch.

Über dieses Handbuch

Dieses Handbuch behandelt die folgenden Themengebiete:

Erste Schritte (Seite 12)

Starten mit Bitdefender Antivirus for Mac und der Benutzeroberfläche.

Schutz gegen Bösartige Software (Seite 17)

Lernen Sie wie Sie Bitdefender Antivirus for Mac anwenden, um sich vor gefährlicher Software zu schützen.

Präferenzen konfigurieren (Seite 39)

Erfahren Sie mehr über die Einstellungen von Bitdefender Antivirus for Mac.

Hilfe und Support (Seite 58)

Beschreibt wie Sie Hilfe bzw. Unterstützung zu dem Produkt erhalten und erhält zusätzlich eine Liste mit den am häufigsten gestellten Fragen (FAQ).

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. WAS IST BITDEFENDER ANTIVIRUS FOR MAC

Bitdefender Antivirus for Mac ist ein leistungsstarker Virenscanner, der alle Arten von Schad-Software („Bedrohungen“) erkennen und entfernen kann:

- Ransomware
- Adware
- Viren
- Spyware
- Trojaner
- Keylogger
- Computerwürmer

Diese App erkennt und entfernt nicht nur Mac-spezifische, sondern auch Windows-spezifische Bedrohungen und verhindert so, dass Sie infizierte Dateien versehentlich an die PCs Ihrer Familie, Freunde und Kollegen weiterleiten.

2. INSTALLATION UND DEINSTALLATION

Dieses Kapital beinhaltet die folgenden Themen:

2.1. Systemanforderungen

Sie können Bitdefender Antivirus for Mac auf Macintosh-Computern mit OS X Yosemite (10.10) oder höher installieren.

Sie benötigen auf Ihrem Mac zudem mindestens 1 GB verfügbaren Speicherplatz auf der Festplatte.

Für die Registrierung und Updates von Bitdefender Antivirus for Mac ist eine aktive Internetverbindung notwendig.

Hinweis
Bitdefender Anti-Tracker und Bitdefender VPN können nur auf Systemen ab macOS 10.12 installiert werden.

So finden Sie heraus, welche macOS-Version und Hardware Sie nutzen
Klicken Sie auf das Apple-Symbol oben linken und wählen Sie **Über diesen Mac**. Daraufhin wird ein Fenster angezeigt, dem Sie die Version Ihres Betriebssystems und andere nützliche Informationen entnehmen können. Klicken Sie auf **Systembericht**, um detaillierte Hardwareinformationen zu erhalten.

2.2. Bitdefender Antivirus for Mac wird installiert

Gehen Sie wie folgt vor, um die Bitdefender Antivirus for Mac-App über Ihr Bitdefender-Konto zu installieren:

1. Als Administrator anmelden.
2. Gehen Sie zu: https://central.bitdefender.com.
3. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Bitdefender-Konto an.

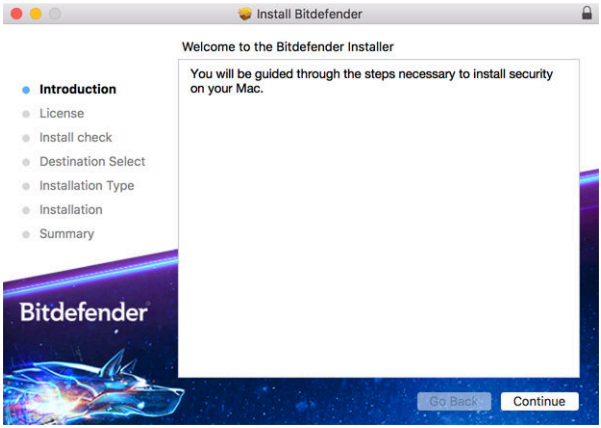
4. Rufen Sie den Bereich **Meine Geräte** auf und klicken Sie auf **SCHUTZ INSTALLIEREN**.
5. Wählen Sie eine der beiden verfügbaren Optionen:
   - **Dieses Gerät schützen**
     a. Wählen Sie diese Option und danach den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, klicken Sie auf die 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.
6. Führen Sie das von Ihnen heruntergeladene Bitdefender aus.
7. Führen Sie die Installationsschritte durch.

2.2.1. Installationsvorgang

So können Sie Bitdefender Antivirus for Mac installieren:

1. Klicken Sie auf die heruntergeladene Datei. Der Installationsassistent wird geöffnet und führt Sie durch den Installationsvorgang.
2. Folgen Sie den Anweisungen des Installationsassistenten.

Schritt 1 - Willkommensfenster



Klicken Sie auf **Fortfahren**.

Schritt 2 - Lesen Sie die Abonnementvereinbarung

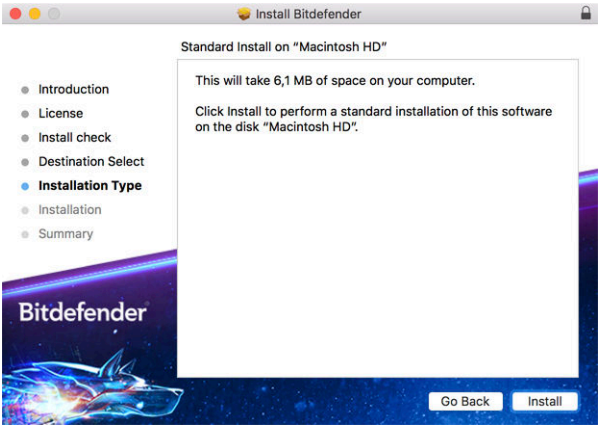
Bevor Sie mit der Installation fortfahren, müssen Sie zunächst der Abonnementvereinbarung zustimmen. Bitte nehmen Sie sich einen Moment Zeit, um die Abonnementvereinbarung zu lesen, da Sie hier die Bedingungen finden, unter denen Sie Bitdefender Antivirus for Mac nutzen dürfen.

In diesem Fenster können Sie auch die Sprache auswählen, in der Sie das Produkt installieren möchten.

Klicken Sie auf **Weiter** und danach auf **Zustimmen**.

> **Wichtig**
> Falls Sie die Nutzungsbedingungen nicht akzeptieren möchten, klicken Sie auf **Weiter** und dann auf **Nicht zustimmen**. Der Installationsvorgang wird dann abgebrochen und der Installationsassistent geschlossen.

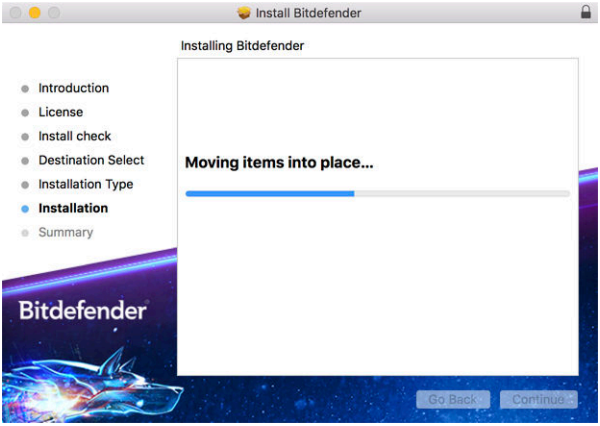
Schritt 3 - Installation starten



Die Installation von Bitdefender Antivirus for Mac erfolgt im Verzeichnis `Macintosh HD/Library/Bitdefender` . Diesen Installationspfad können Sie nicht ändern.

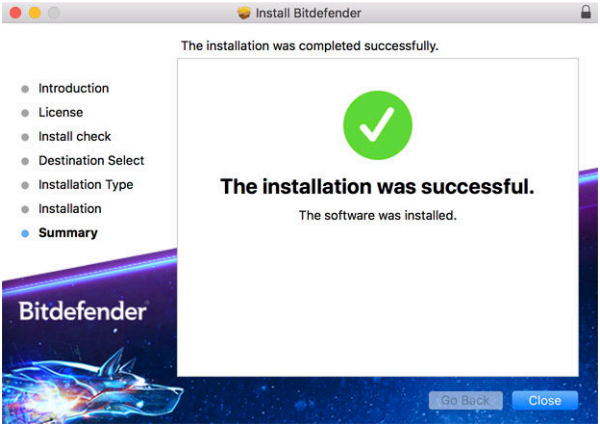
Klicken Sie auf **Installieren**, um die Installation zu starten.

Schritt 4 - Bitdefender Antivirus for Mac installieren



Warten Sie, bis die Installation abgeschlossen ist und klicken Sie auf **Weiter**.

Schritt 5 - Fertigstellung



Klicken Sie auf **Schließen**, um das Installationsfenster zu schließen.

Damit ist der Installationsvorgang abgeschlossen.

Wichtig

- Wenn Sie Bitdefender Antivirus for Mac unter macOS High Sierra 10.13.0 oder einer neueren Version installieren, erscheint die Benachrichtigung **Systemerweiterung blockiert**. Diese Benachrichtigung informiert Sie darüber, dass die von Bitdefender signierten Erweiterungen blockiert wurden und manuell aktiviert werden müssen. Klicken Sie auf OK, um fortzufahren. Klicken Sie in dem von Bitdefender Antivirus for Mac angezeigten Fenster auf den Link **Sicherheit & Datenschutz**. Klicken Sie unten im Fenster auf **Zulassen** oder wählen Sie die Bitdefender SRL aus der Liste und klicken Sie dann auf **OK**.
- Wenn Sie Bitdefender Antivirus for Mac unter macOS Mojave 10.14 oder einer neueren Version installieren, erscheint ein neues Fenster, das Sie darüber informiert, dass Sie **Bitdefender vollständigen Festplattenzugriff gewähren** und **Bitdefender das Laden erlauben** müssen. Folgen Sie den Anweisungen auf dem Bildschirm, um das Produkt ordnungsgemäß zu konfigurieren.

2.3. Bitdefender Antivirus for Mac deinstallieren

Bitdefender Antivirus for Mac ist eine komplexe Anwendung und kann nicht auf herkömmliche Weise deinstalliert werden, indem das Symbol für die Anwendung aus dem Verzeichnis **Anwendungen** in den Papierkorb gezogen wird.

Gehen Sie wie folgt vor, um Bitdefender Antivirus for Mac zu entfernen:

1. Öffnen Sie **Finder** und wählen Sie den **Programme**-Ordner.
2. Öffnen Sie den Bitdefender-Ordner unter Anwendungen und doppelklicken Sie dann auf **BitdefenderUninstaller**.
3. Select the preferred uninstall option.

   Hinweis
   Wenn Sie nur die Bitdefender VPN-App entfernen möchten, klicken Sie **VPN deinstallieren**.

4. Klicken Sie auf **Deinstallieren**, und warten Sie, bis der Vorgang abgeschlossen ist.
5. Klicken Sie zum Abschluss auf **Schließen**.

Wichtig

Ist ein Fehler aufgetreten, so können Sie die Kundenbetreuung von Bitdefender wie in Hier wird Ihnen geholfen (Seite 58) beschrieben, kontaktieren.

3. ERSTE SCHRITTE

Dieses Kapitel enthält die folgenden Themen:

3.1. Bitdefender Antivirus for Mac öffnen

Sie können Bitdefender Antivirus for Mac auf verschiedene Weisen öffnen.

- Klicken Sie im Launchpad auf das "Bitdefender Antivirus for Mac"-Symbol.
- Klicken Sie auf das Symbol  in der Menüleiste und wählen Sie **Benutzeroberfläche öffnen**.
- Öffnen Sie ein Finder-Fenster, wählen Sie Anwendungen und doppelklicken Sie auf das **Bitdefender Antivirus for Mac**-Symbol.

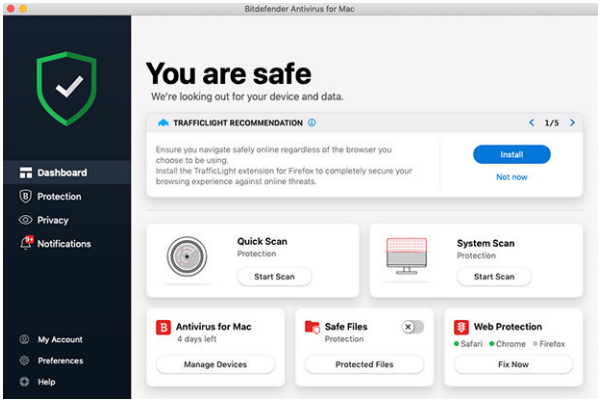
Wichtig

Wenn Sie Bitdefender Antivirus for Mac zum ersten Mal unter macOS Mojave 10.14 oder einer neueren Betriebssystemversion öffnen, wird eine Sicherheitsempfehlung angezeigt. Der Grund dafür ist, dass unsere Software bestimmte Berechtigungen benötigt, um Ihr System vollständig scannen zu können. Um diese Berechtigungen zu erteilen, müssen Sie als Administrator angemeldet sein. Gehen Sie dazu wie folgt vor:

1. Klicken Sie auf den Link **Systemeinstellungen**.
2. Klicken Sie auf das -Symbol und geben Sie dann Ihre Administratoranmeldeinformationen ein.
3. Ein neues Fenster wird geöffnet. Ziehen Sie die Datei **BDLDaemon** mit der Maus auf die Liste der zugelassenen Apps.

3.2. Das Hauptfenster

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



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

Die Statusleiste oben im Fenster informiert Sie mit eindeutigen Meldungen und aussagekräftigen Farben über den Sicherheitsstatus des Systems. Wenn Bitdefender Antivirus for Mac keine Warnmeldungen für Sie hat, bleibt die Statusleiste grün. Wenn ein Sicherheitsproblem erkannt wurde, ändert die Statusleiste ihre Farbe zu rot. Detaillierte Informationen zu Problemen und deren Behebung finden Sie unter Alle beheben (Seite 29).

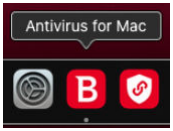
Um einen wirksamen Betrieb und noch besseren Schutz bei Ihren verschiedenen Aktivitäten sicherzustellen, fungiert der **Bitdefender Autopilot** als Ihr persönlicher Sicherheitsberater. Je nachdem, was Sie gerade machen - egal, ob Sie arbeiten oder gerade Online-Zahlungen durchführen - der Bitdefender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

in Ihrer Bitdefender Antivirus for Mac-App kennen und können umfassend davon profitieren.

Über das Navigationsmenü links können Sie die Bitdefender-Abschnitte für die detaillierte Konfiguration und erweiterte Verwaltungsaufgaben (in den Reitern **Schutz** und **Privatsphäre**), Benachrichtigungen, Ihr **Bitdefender-Benutzerkonto** und den Bereich **Einstellungen** aufrufen. Außerdem können Sie sich mit uns in Verbindung setzen (im Reiter **Hilfe**), falls Sie Fragen haben oder unerwartete Probleme auftreten.

3.3. Dock-Symbol der App

Das Bitdefender Antivirus for Mac-Symbol wird im Dock angezeigt, sobald Sie die Anwendung öffnen. Über das Symbol im Dock können Sie Dateien und Ordner ganz einfach auf Bedrohungen scannen. Ziehen Sie einfach die Datei oder den Ordner auf das Dock-Symbol und der Scan wird sofort gestartet.



3.4. Navigationsmenü

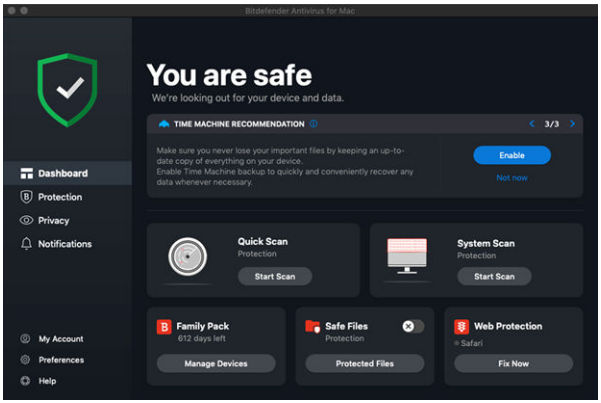
Auf der linken Seite der Bitdefender-Oberfläche finden Sie das Navigationsmenü mit Schnellzugriff auf alle Bitdefender-Funktionen, die Sie für den Umgang mit Ihrem Produkt benötigen. In diesem Bereich gibt es die folgenden Reiter:

- **Dashboard**. Von hier aus können Sie Sicherheitsprobleme schnell beheben, von Ihren Systemanforderungen und Nutzungsverhalten abgeleitete Empfehlungen anzeigen, Schnellaktionen ausführen und Ihr Bitdefender-Konto aufrufen, um die Geräte zu verwalten, die Sie Ihrem Bitdefender-Abonnement hinzugefügt haben.
- **Schuz**. Von hier aus können Sie Virenschutz-Scans starten, Dateien zur Ausnahmeliste hinzufügen, Dateien und Anwendungen vor Ransomware-Angriffen schützen, Ihre Time Machine-Backups sichern und den Schutz beim Surfen im Internet konfigurieren.

- **Privatsphäre**. Von hier aus können Sie die Bitdefender VPN-App öffnen und die Anti-Tracker-Erweiterung in Ihrem Webbrowser installieren.
- **Benachrichtigungen**. Hier finden Sie Details zu den Aktionen, die für gescannte Dateien durchgeführt wurden.
- **Mein Konto**. Hier finden Sie das Bitdefender-Konto und das Abonnement, über die Ihr Gerät geschützt ist. Hier können Sie bei Bedarf auch Ihr Konto wechseln.
- **Einstellungen**. Hier können Sie die Bitdefender-Einstellungen konfigurieren.
- **Hilfe**. Wenn Sie Unterstützung beim Umgang mit Ihrem Bitdefender-Produkt benötigen, können Sie sich von hier aus an den technischen Support wenden. Von hier aus können Sie uns zudem Ihr Feedback schicken, um uns bei der Verbesserung des Produkts zu helfen.

3.5. Dark Mode

Um Ihre Augen bei Nachtarbeiten oder in einer lichtarmen Umgebung vor Blendung und Licht zu schützen, unterstützt Bitdefender Antivirus for Mac den Dark Mode für Mojave 10.14 und höher. Die Farben der Benutzeroberfläche wurden so optimiert, dass Sie Ihren Mac verwenden können, ohne Ihre Augen anzustrengen. Die Bitdefender Antivirus for Mac-Benutzeroberfläche passt sich an die Darstellungseinstellungen Ihres Geräts an.


Bitdefender Antivirus for Mac
You are safe
We're looking out for your device and data.
TIME MACHINE RECOMMENDATION
3/3
Make sure you never lose your important files by keeping an up-to-date copy of everything on your device.
Enable Time Machine backup to quickly and conveniently recover any data whenever necessary.
Enable
Not now
Dashboard
Protection
Privacy
Notifications
Quick Scan
Protection
Start Scan
System Scan
Protection
Start Scan
Family Pack
612 days left
Manage Devices
Safe Files
Protection
Protected Files
Web Protection
Safari
Fix Now
My Account
Preferences
Help

4. SCHUTZ GEGEN BÖSARTIGE SOFTWARE

Dieses Kapitel enthält die folgenden Themen:

4.1. Empfohlene Vorgehensweisen

Um Ihr System vor Bedrohungen zu schützen und eine versehentliche Infizierung anderer Systeme zu verhindern, sollten Sie folgende Empfehlungen beachten:

- Lassen Sie **Bitdefender Shield** aktiviert, damit Systemdateien automatisch von Bitdefender Antivirus for Mac gescannt werden können.
- Halten Sie Ihr Bitdefender Antivirus for Mac-Produkt mit den neusten Bedrohungsinformationen und Produktupdates immer aktuell.
- Überprüfen und beheben Sie die von Bitdefender Antivirus for Mac aufgelisteten Probleme regelmäßig. Detaillierte Informationen finden Sie im Kapitel Alle beheben (Seite 29).
- Im detaillierten Ereignisprotokoll finden Sie alle Aktionen, die Bitdefender Antivirus for Mac auf Ihrem Computer durchgeführt hat.

Alle Ereignisse, die sich auf Ihr System oder Ihre Daten auswirken, werden als neue Nachricht in den Bitdefender-Benachrichtigungen angezeigt. Weitere Details finden Sie unter Benachrichtigungen (Seite 31).

- Darüber hinaus sollten Sie folgende Empfehlungen berücksichtigen:
  - Sie sollten grundsätzlich alle Dateien scannen, die Sie von externen Speichern (z.B. USB-Sticks oder CDs) herunterladen, insbesondere wenn Ihnen die Quelle nicht bekannt ist.
  - Bei DMG-Dateien sollten diese zunächst gemountet und dann ihr Inhalt (die Dateien im gemounteten Volume/Image) gescannt werden.

  Sie können Dateien, Ordner oder Volumes ganz einfach scannen, indem Sie sie per Drag & Drop auf das Anwendungsfenster oder das Dock-Symbol von Bitdefender Antivirus for Mac ziehen.

Es sind keine weitere Konfigurationen oder Aktionen erforderlich. Sie können jedoch bei Bedarf Anpassungen an den Einstellungen vornehmen. Weitere Informationen finden Sie im Kapitel Präferenzen konfigurieren (Seite 39).

4.2. Ihren Mac scannen

Die **Bitdefender Shield**-Funktion überwacht alle installierten Anwendungen auf Aktionen, die auf Bedrohungen hindeuten, und verhindert, dass neue Bedrohungen auf Ihr System gelangen. Darüber hinaus können Sie Ihren Mac oder einzelne Dateien jederzeit nach Bedarf scannen.

Sie können Dateien, Ordner oder Volumes ganz einfach scannen, indem Sie sie per Drag & Drop auf das Anwendungsfenster oder das Dock-Symbol von Bitdefender Antivirus for Mac ziehen. Daraufhin wird der Scan-Assistent angezeigt, um Sie durch den Scan-Vorgang zu führen.

Sie können einen Scan wie folgt starten:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Wechseln Sie zum Reiter **Virenschutz**.
3. Klicken Sie auf einen der drei Scan-Schaltflächen, um den gewünschten Scan zu starten.

- **Quick Scan** - überprüft die sensibelsten Verzeichnisse Ihres Systems (beispielsweise die Verzeichnisse mit Dokumenten, Downloads, Mail-Downloads und temporären Dateien eines Benutzers) auf Bedrohungen.
- **System-Scan** - durchsucht das gesamte System eingehend nach möglichen Bedrohungen. Alle eingebundenen Dateisysteme werden ebenfalls gescannt.

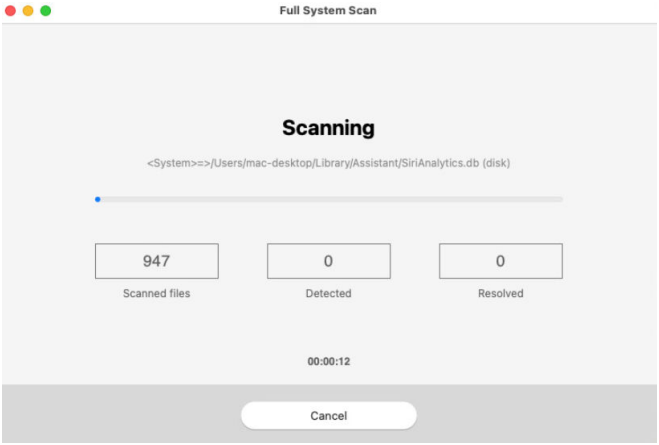
  > **Hinweis**
  > Je nach Größe Ihrer Festplatte kann ein vollständiger System-Scan einige Zeit in Anspruch nehmen (bis zu einer Stunde und mehr). Um die Systemleistung nicht zu beeinträchtigen, sollte diese Aufgabe nicht zeitgleich mit anderen ressourcenintensiven (z.B. Videobearbeitung) Aufgaben ausgeführt werden.
  >
  > Falls gewünscht, können Sie bestimmte Laufwerke vom Scan ausschließen, indem Sie sie in im Fenster Schutz zur Liste der **Ausnahmen** hinzufügen.

- **Benutzerdefinierter Scan** - hiermit können einzelne Dateien, Verzeichnisse etc. auf Bedrohungen geprüft werden.

Sie können über das Dashboard auch einen System-Scan oder einen Quick Scan starten.

4.3. Scan-Assistent

Sobald Sie einen Scan starten, öffnet sich der Bitdefender Antivirus for Mac-Scan-Assistent.



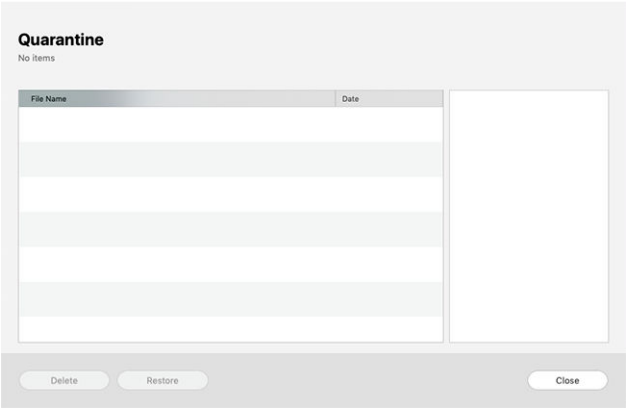
Während eines Scans werden Informationen zu gefundenen und behobenen Bedrohungen in Echtzeit angezeigt.

Warten Sie bis Bitdefender Antivirus for Mac den Prüfvorgang beendet hat.

> **Hinweis**
> Der Scan-Vorgang kann, abhängig von der Größe Ihrer Festplatte, eine Weile dauern.

4.4. Quarantäne

Mit Bitdefender Antivirus for Mac können infizierte oder verdächtige Dateien in einem sicheren Bereich, der Quarantäne, isoliert werden. Bedrohungen in Quarantäne können keinen Schaden anrichten, da sie dort nicht geöffnet oder ausgeführt werden können.



Der Bereich Quarantäne zeigt alle Dateien an, die sich zur Zeit im Quarantäne-Ordner befinden.

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

So können Sie eine Liste mit allen zur Quarantäne hinzugefügten Objekten anzeigen:

1. Klicken **Schutz** im Navigationsmenü der Bitdefender-Benutzeroberfläche.
2. Klicken Sie im Bereich **Quarantäne** auf **Öffnen**.

4.5. Bitdefender Shield (Echtzeitschutz)

Bitdefender bietet Ihnen Echtzeitschutz vor einer Vielzahl an Bedrohungen, indem es alle installierten Apps und ihre jeweiligen Updates sowie alle neuen und veränderten Dateien scannt.

So können Sie den Echtzeitschutz deaktivieren:

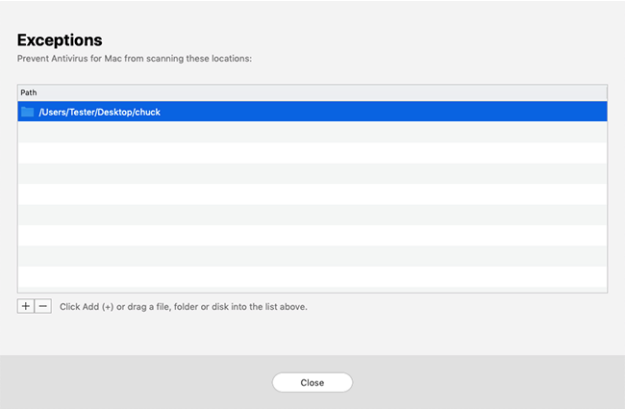
1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Einstellungen**.
2. Deaktivieren Sie **Bitdefender Shield** im Fenster **Schutz**.

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.

4.6. Scan-Ausnahmen

Wenn Sei möchten können Sie Bitdefender Antivirus for Mac so einstellen, dass spezielle Dateien, Ordner oder auch ein ganzer Datenträger, nicht gescannt werden. Zum Beispiel könnten Sie vom Scannen ausschließen:

- Dateien die fälschlicherweise als infiziert identifiziert wurden (bekannt als "false positives")
- Dateien die Scanfehler verursachen
- Backup-Laufwerke



In der Ausnahmeliste sind alle Pfade aufgeführt, die vom Scan ausgenommen wurden.

So können Sie die Ausnahmeliste aufrufen:

1. Klicken **Schutz** im Navigationsmenü der Bitdefender-Benutzeroberfläche.
2. Klicken Sie im Bereich **Ausnahmen** auf **Öffnen**.

Es gibt zwei Wege um eine Scan-Ausnahme einzurichten:

- Fügen Sie Dateien, Ordner oder Volumes per Drag & Drop zur Ausnahmeliste hinzu.
- Klicken Sie auf das Pluszeichen (+) unterhalb der Ausnahmeliste. Wählen Sie danach die Datei, den Ordner oder das Laufwerk, das vom Scan ausgeschlossen werden soll.

Um eine Scan-Ausnahme zu entfernen, wählen Sie den entsprechenden Eintrag aus der Liste aus und klicken Sie auf das Minuszeichen (-) unterhalb der Ausnahmeliste.

4.7. Internet-Schutz

Bitdefender Antivirus for Mac nutzt die Linkchecker-Erweiterungen, um Ihnen sicheres Surfen im Internet zu ermöglichen. Die Linkchecker-Erweiterungen lesen, verarbeiten und filtern den gesamten Datenverkehr und blockieren dabei schädlichen Inhalte.

Die Erweiterungen lassen sich in die folgenden Browser integrieren: Mozilla Firefox, Google Chrome and Safari.

4.7.1. Aktivieren der TrafficLight-Erweiterungen

So können Sie die TrafficLight-Erweiterungen aktivieren:

1. Klicken Sie in der **Internet-Schutz**-Kachel im Dashboard auf **Jetzt lösen**.
2. Das Fenster **Internet-Schutz** wird geöffnet.
   Der auf Ihrem System installierte Browser wird erkannt und angezeigt. Klicken Sie zur Installation der TrafficLight-Erweiterung in Ihrem Browser auf **Erweiterung herunterladen**.
3. Sie werden umgeleitet auf:
   https://www.bitdefender.com/solutions/trafficlight.html
4. Wählen Sie **Kostenloser Download**.
5. Folgen Sie den Anweisungen, um die TrafficLight-Erweiterung für Ihren Browser zu installieren.

4.7.2. Verwalten von Erweiterungseinstellungen

Ihnen steht eine große Auswahl an Funktionen zur Verfügung, die Sie vor allen möglichen Bedrohungen im Internet schützen. Sie können sie

aufrufen, indem Sie auf das TrafficLight-Symbol neben Ihren Browser-Einstellungen und danach auf **Einstellungen**-Schaltfläche klicken:

- **Bitdefender TrafficLight-Einstellungen**
  - Internet-Schutz - Verhindert, dass Sie Websites aufrufen, die zur Verbreitung von Malware sowie von Phishing- und Betrugsversuchen eingesetzt werden.
  - Suchberater - Warnt Sie schon in Ihren Suchergebnissen vor gefährlichen Websites.

- **Ausnahmen**
  Wenn Sie die Website, die Sie zu den Ausnahmen hinzufügen möchten, bereits aufgerufen haben, klicken Sie auf **Aktuelle Website zur Liste hinzufügen**.
  Wenn Sie eine weitere Website hinzufügen möchten, geben Sie deren Adresse in das entsprechende Feld ein und klicken Sie auf .
  Es wird keine Warnmeldung mehr angezeigt, auch wenn von den ausgenommenen Seiten eine Bedrohung ausgeht. Sie sollten dieser Liste nur Website hinzufügen, denen Sie uneingeschränkt vertrauen.

4.7.3. Seitenbewertung und Warnungen

Abhängig von der Linkchecker-Einstufung für die Webseite, die sie gerade besuchen, wird eines der folgenden Symbole in diesem Bereich eingeblendet:

Diese Seite ist sicher und kann aufgerufen werden. Sie können Ihre Arbeit fortsetzen.

Diese Webseite könnte gefährliche Inhalte haben. Lassen Sie Vorsicht walten, wenn Sie sie dennoch aufrufen möchten.

Sie sollten die Webseite sofort verlassen, da sie Malware oder andere Bedrohungen enthält.

In Safari sind die TrafficLight-Symbole schwarz hinterlegt.

4.8. Anti-Tracker

Viele der von Ihnen aufgerufenen Websites verwenden Tracker, um Informationen über Ihr Surf-Verhalten zu sammeln, entweder um sie mit anderen Unternehmen zu teilen oder um Werbeanzeigen einzublenden,

die für Sie relevanter sind. Website-Betreiber verwenden die hierdurch erzielten Einnahmen, um Ihnen kostenlose Inhalte anzubieten oder den eigenen Betrieb aufrechtzuerhalten. Das Sammeln dieser Informationen kann sich auch auf Ihre Surf-Geschwindigkeit auswirken und übermäßig Bandbreite in Anspruch nehmen.

Durch Aktivierung der Bitdefender Anti-Tracker-Erweiterung in Ihrem Browser verhindern Sie Tracking, sodass Ihre Daten während des Surfens im Netz privat bleiben. Darüber hinaus können Websites schneller geladen werden.

Die Bitdefender-Erweiterung ist mit den folgenden Web-Browsern kompatibel:

- Google Chrome
- Mozilla Firefox
- Safari

Die von uns erkannten Tracker sind in die folgenden Kategorien unterteilt:

- **Werbung** - Dient der Analyse von Website-Verkehr, von Nutzerverhalten oder von Datenverkehrsmustern von Website-Besuchern.
- **Kundeninteraktion** - Dient der Messung der Benutzerinteraktion mit verschiedenen Eingabemöglichkeiten wie Chat oder Support.
- **Wesentlich** - Dient der Überwachung kritischer Webseiten-Funktionen.
- **Site Analytics** - Dient der Sammlung von Daten über die Nutzung von Webseiten.
- **Social Media** - Dient der Überwachung von Social-Media-Zielgruppen sowie der Aktivitäten und Nutzerbindung über verschiedene Social-Media-Plattformen.

4.8.1. Aktivieren von Bitdefender Anti-Tracker

So können Sie die Bitdefender Anti-Tracker-Erweiterung in Ihrem Browser aktivieren:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Privatsphäre**.
2. Wechseln Sie zum Reiter **Anti-tracker**.

3. Klicken Sie neben dem Browser, für den Sie die Erweiterung aktivieren möchten, auf **Erweiterung aktivieren**.

4.8.2. Anti-Tracker-Benutzeroberfläche

Nach Aktivierung der Bitdefender Anti-Tracker-Erweiterung erscheint das Symbol neben der Suchleiste in Ihrem Webbrowser. Jedes Mal, wenn Sie eine Website besuchen, wird auf dem Symbol ein Zähler angezeigt, der Aufschluss über erkannte und blockierte Tracker gibt. Um weitere Details zu den blockierten Trackern anzuzeigen, klicken Sie auf das Symbol, um die Benutzeroberfläche zu öffnen. Neben der Anzahl der blockierten Tracker können Sie die Ladezeit der Seite und die Kategorien der erkannten Tracker einsehen. Klicken Sie auf die gewünschte Kategorie, um die Liste der Websites anzuzeigen, die Sie tracken.

Um Bitdefender davon abzuhalten, Tracker auf der aktuell von Ihnen besuchten Website zu blockieren, klicken Sie auf **Schutz für diese Website anhalten**. Diese Einstellung gilt nur, solange die Website geöffnet ist und wird beim Schließen der Website in den Ausgangszustand zurückgesetzt.

Um Trackern aus einer bestimmten Kategorie die Überwachung Ihrer Aktivität zu erlauben, klicken Sie auf die gewünschte Aktivität, und klicken Sie dann auf die entsprechende Schaltfläche. Klicken Sie erneut auf die gleiche Schaltfläche, falls Sie Ihre Meinung ändern.

4.8.3. Deaktivieren von Bitdefender Anti-Tracker

So können Sie die Bitdefender Anti-Tracker-Erweiterung in Ihrem Browser deaktivieren:

1. Öffnen Sie Ihren Internet-Browser.
2. Klicken Sie auf das -Symbol neben der Adressleiste in Ihrem Webbrowser.
3. Klicken Sie oben rechts auf das -Symbol.
4. Verwenden Sie zum Deaktivieren den entsprechenden Schalter.
   Das Bitdefender-Symbol wird grau.

4.8.4. Erlauben von Tracking auf einer Website

Wenn Sie beim Besuch einer bestimmten Website das Tracking erlauben möchten, können Sie die entsprechende Adresse wie folgt zu den Ausnahmen hinzufügen:

1. Öffnen Sie Ihren Webbrowser.
2. Klicken Sie auf das -Symbol neben der Suchleiste.
3. Drücke den Symbol in der oberen rechten Ecke.
4. Wenn Sie sich auf der Website befinden, die Sie zu Ausnahmen hinzufügen möchten, klicken Sie auf **Aktuelle Website zur Liste hinzufügen**.
   Wenn Sie eine weitere Website hinzufügen möchten, geben Sie deren Adresse in das entsprechende Feld ein und klicken Sie dann auf .

4.9. Safe Files

Bei Ransomware handelt es sich um Schadsoftware, die anfällige Systeme infiziert und den Zugriff darauf sperrt. Von den Benutzern wird dann für die Freigabe ihrer Daten ein Lösegeld erpresst. Diese Schadsoftware geht intelligent vor und zeigt Benutzern gefälschte Warnmeldungen an, um sie in Angst zu versetzen und sie dazu zu bringen, das geforderte Geld zu zahlen.

Durch den Einsatz neuester Technologien stellt Bitdefender die Integrität des Systems sicher. Kritische Systembereiche werden vor Ransomware-Angriffen geschützt, ohne dabei das System zu beeinträchtigen. Um zu verhindern, dass nicht vertrauenswürdige Anwendungen auf Ihre Dokumente, Fotos oder Videos zugreifen, bietet Ihnen Bitdefender Safe Files Ihnen die Möglichkeit, Ihre persönlichen Dateien in einem geschützten Umfeld abzulegen und selbst festzulegen, welche Apps autorisiert sind, Änderungen an diesen geschützten Dateien vorzunehmen.

So können Sie auch zu einem späteren Zeitpunkt weitere Dateien zur geschützten Umgebung hinzufügen:

1. Klicken **Schutz** im Navigationsmenü der Bitdefender-Benutzeroberfläche.
2. Wechseln Sie zum Reiter **Ransomware-Schutz**.
3. Klicken Sie im Bereich Sichere Dateien auf **Geschützte Dateien**.
4. Klicken Sie auf das Pluszeichen (+) unterhalb der Liste mit den geschützten Dateien. Wählen Sie danach die Datei, den Ordner oder das Laufwerk aus, das Sie vor dem Zugriff durch Ransomware schützen möchten.

Um Systembeeinträchtigungen zu vermeiden, sollten Sie nicht mehr als 30 Ordner hinzufügen oder mehrere Dateien in einem Ordner speichern.

Die Ordner Bilder, Dokumente, Desktop und Downloads werden standardmäßig vor Angriffen geschützt.

> **Hinweis**
> Benutzerdefinierte Ordner können nur für aktuelle Benutzer geschützt werden. Externe Laufwerke sowie System- und Anwendungsdateien können der Schutzumgebung nicht hinzugefügt werden.

Sie werden informiert, sobald eine unbekannte Anwendung mit ungewöhnlichen Verhalten versucht, die von Ihnen hinzugefügten Dateien zu verändern. Klicken Sie auf **Zulassen** oder **Blockieren**, um sie zur Liste der **verwalteten Anwendungen** hinzuzufügen.

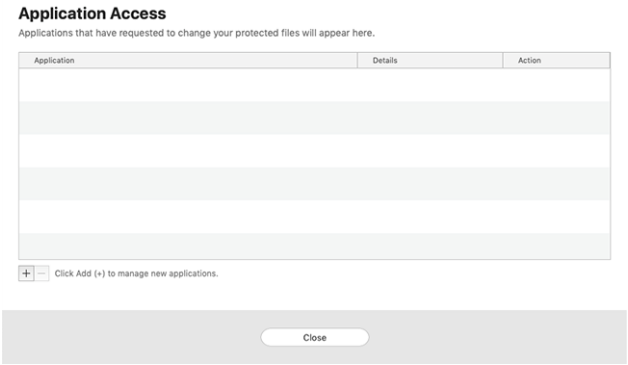
4.9.1. Anwendungszugriff

Anwendungen, die versuchen, geschützte Dateien zu verändern oder zu löschen, können als potenziell unsicher markiert und zur Liste der blockierten Anwendungen hinzugefügt werden. Falls eine solche Anwendung blockiert wurde und Sie sich sicher sind, dass ihr Verhalten normal ist, können Sie ihre Ausführung wie folgt zulassen:

1. Klicken **Schutz** im Navigationsmenü der Bitdefender-Benutzeroberfläche.
2. Wähle aus **Anti-Ransomware** Tab.
3. Klicken Sie im Bereich Sichere Dateien auf **Anwendungszugriff**.
4. Ändern Sie den Status neben der blockierten App auf Erlauben.

Ebenso können Sie den Status zugelassener Anwendungen auf blockiert setzen.

Nutzen Sie Drag&Drop oder klicken Sie auf das Pluszeichen (+), um weitere Apps zur Liste hinzuzufügen.



4.10. Time-Machine-Schutz

Der Bitdefender Time Machine Protection bietet zusätzliche Sicherheit für Ihr Backup-Laufwerk und alle darauf gespeicherten Dateien, indem es den Zugriff durch externe Quellen verhindert. Werden Dateien in Ihrem Time-Machine-Laufwerk von Ransomware verschlüsselt, können Sie sie auch ohne Lösegeldzahlung wiederherstellen.

Falls Sie Objekte aus einer Time-Machine-Sicherung wiederherstellen müssen, finden Sie die entsprechende Anleitung auf der Apple-Support-Seite.

4.10.1. Aktivierung und Deaktivierung des Time-Machine-Schutzes

So können Sie den Time-Machine-Schutz aktivieren oder deaktivieren:

1. Klicken Sie im Navigationsmenü der **Bitdefender-Benutzeroberfläche** auf **Schutz**.
2. Wähle aus **Anti-Ransomware** Tab.
3. Aktivieren oder deaktivieren Sie den Schalter **Time-Machine-Schutz**.

4.11. Alle beheben

Bitdefender Antivirus for Mac spürt automatisch mögliche Probleme, die die Sicherheit Ihres Systems beeinflussen können, auf und informiert Sie. So können Sicherheitsrisiken einfach und frühzeitig behoben werden.

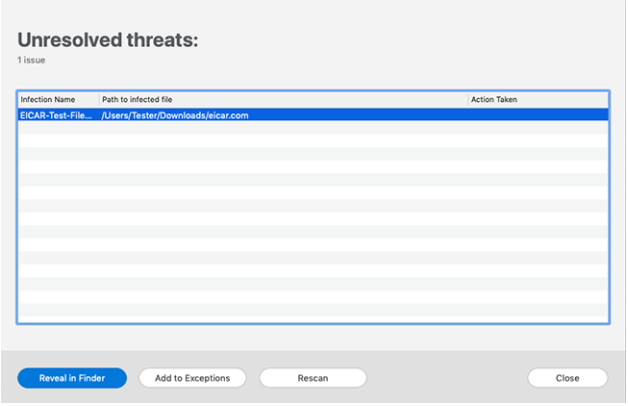
Beheben Sie die in Bitdefender Antivirus for Mac angezeigten Probleme, um schnell und einfach den optimalen Schutz für Ihr System und Ihre Daten sicherzustellen.

Zu den erkannten Problemen gehören:

- Das neueste Update der Bedrohungsinformationen wurde nicht von unserer Servern heruntergeladen.
- Auf Ihrem System wurden Bedrohungen gefunden, die das Produkt nicht automatisch beheben kann.
- Der Echtzeitschutz ist deaktiviert.

Um erkannte Probleme zu überprüfen und zu beheben:

1. Liegen keine Warnungen in Bitdefender vor, ist die Statusleiste grün. Wird ein Sicherheitsproblem gefunden, wechselt die Farbe der Statusleiste zu rot.
2. Überprüfen Sie die Beschreibung für weitere Informationen.
3. Wird ein Problem erkannt, können Sie mit einem Klick auf die entsprechende Schaltfläche Gegenmaßnahmen einleiten.



Die Liste der nicht behobenen Bedrohungen wird nach jedem System-Scan aktualisiert. Dies geschieht unabhängig davon, ob der Scan automatisch im Hintergrund durchgeführt oder von Ihnen angestoßen wurde.

Für nicht beseitigte Bedrohungen sind die folgenden Aktionen verfügbar:

- **Manuell löschen**. Führen Sie diese Aktion aus, um Infektionen manuell zu entfernen.
- **Zu den Ausnahmen hinzufügen**. Diese Aktion ist nicht für Bedrohungen verfügbar, die in Archiven gefunden werden.

4.12. Benachrichtigungen

Bitdefender führt ein detailliertes Ereignisprotokoll über alle Aktivitäten der Software auf Ihrem Computer. 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 im System 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.

4.13. Updates

Jeden Tag werden neue Bedrohungen entdeckt und identifiziert. Deshalb ist es so wichtig, Bitdefender Antivirus for Mac über Updates ständig auf dem neuesten Stand zu halten.

Die Aktualisierung der Bedrohungsinformationen wird „on the fly" durchgeführt. Das bedeutet, dass die zu aktualisierenden Dateien schrittweise ersetzt werden. Dadurch wird die Funktionalität des Produkts nicht eingeschränkt und Ihr System zu keiner Zeit gefährdet.

- Wenn Bitdefender Antivirus for Mac up-to-date ist, spürt die Software die neuesten Threats auf und heilt infizierte Dateien.
- Wenn Bitdefender Antivirus für Mac nicht auf dem neuesten Stand ist, kann es die neuesten von Bitdefender Labs entdeckten Bedrohungen nicht erkennen und entfernen.

4.13.1. Benutzergesteuertes Update

Ein manuelles Update können Sie jederzeit durchführen.

Für regelmäßige Updates und Downloads ist eine aktive Internetverbindung nötig.

Führen Sie folgende Schritte für ein manuelles Update durch:

1. Klicken Sie auf die Schaltfläche **Aktionen** in der Menüleiste.
2. Wählen Sie **Update der Bedrohungsinformationen**.

Alternativ können Sie ein Update auch manuell anfordern, indem Sie CMD + U drücken.

Der Update-Fortschritt und die downgeloadeten Dateien werden eingeblendet.

4.13.2. Updates über einen Proxy Server

Bitdefender Antivirus for Mac kann nur über Proxy-Server aktualisiert werden, bei denen keine Authentifizierung erforderlich ist. Sie müssen dafür keine Programmeinstellungen konfigurieren.

Wenn Ihre Internetverbindung über einen Proxy-Server läuft, der eine Autorisierung verlangt, müssen Sie regelmäßig zu einer direkten Internetverbindung wechseln, um die neuesten Bedrohungsinformationen herunterladen zu können.

4.13.3. Upgrade auf eine neue Version durchführen

Von Zeit zu Zeit veröffentlichen wir Produkt-Updates, die neue Funktionen bringen oder bestimmte Aspekte der Software verbessern oder Probleme beheben. Bei diesen Updates kann es notwendig werden, das System neu zu starten, um die Installation neuer Dateien zu ermöglichen. Falls ein Update einen Neustart erforderlich macht, wird Bitdefender Antivirus for Mac standardmäßig bis zum Neustart des Systems die bereits vorhandenen Dateien nutzen. So beeinträchtigt der Aktualisierungsprozess den Benutzer nicht bei seiner Arbeit.

Ein Pop-up-Fenster fordert Sie auf das System neu zu starten, sobald das Update abgeschlossen wurde. Fall Sie diese Benachrichtigung verpassen, können Sie das System manuell neu starten oder in der Menüleiste auf **Für das Upgrade neu starten** klicken.

4.13.4. Suche nach Informationen über Bitdefender Antivirus for Mac

Informationen zur installierten Bitdefender Antivirus for Mac-Version finden Sie im Bereich **Info über**. Hier können Sie die Abonnementvereinbarung sowie die Datenschutzerklärung aufrufen und lesen sowie die Open-Source-Lizenzen anzeigen.

So rufen Sie das Fenster „Info über“ auf:

1. Öffnen Sie Bitdefender Antivirus for Mac.
2. Klicken Sie in der Menüleiste auf Bitdefender Antivirus for Mac und wählen Sie **Über Antivirus for Mac**.

5. VPN

Dieses Kapitel enthält die folgenden Themen:

5.1. Über VPN

Mit Bitdefender VPN schützen Sie Ihre Daten bei Verbindungen mit ungesicherten WLAN-Netzwerken wie zum Beispiel in Flughäfen, Einkaufszentren, Cafés oder Hotels. So vermeiden Sie bedauerliche Vorfälle wie den Diebstahl Ihrer persönlichen Daten oder Versuche, Ihre Geräte-IP-Adresse für Hacker offenzulegen.

Sie können die VPN-App über Ihr Bitdefender-Produkt installieren. Nutzen Sie sie immer dann, wenn Sie Ihre Verbindung zusätzlich absichern wollen. Das VPN dient als Tunnel zwischen Ihrem Gerät und dem Netzwerk, mit dem Sie sich verbinden. Ihre Verbindung wird abgesichert, Ihren Daten werden professionell nach Bankenstandard verschlüsselt und Ihre IP-Adresse bleibt jederzeit unsichtbar. Ihr Datenverkehr wird über einen speziellen Server weitergeleitet, was es unmöglich macht, Ihr Gerät unter den unzähligen anderen Geräten zu identifizieren, die ebenfalls unsere Dienste in Anspruch nehmen. Darüber hinaus können Sie mit Bitdefender VPN im Internet auch auf solche Inhalte zugreifen, die üblicherweise regionalen Zugangsbeschränkungen unterliegen.

Hinweis

In manchen Ländern wird Internetzensur betrieben. Aus diesem Grund ist die Nutzung von VPNs hier gesetzlich verboten. Um rechtliche Konsequenzen zu vermeiden, wird Ihnen bei der ersten Nutzung der -VPN-App eine Warnmeldung angezeigt. Durch die weitere Nutzung der App bestätigen Sie, dass Sie sich aller einschlägigen Rechtsvorschriften in Ihrem Land sowie der möglichen Risiken, denen Sie sich aussetzen, bewusst sind.

5.2. Öffnen des VPN

Sie haben drei Optionen zum Öffnen der Bitdefender VPN-App:

- Klicken Sie im Navigationsmenü der **Bitdefender-Benutzeroberfläche** auf **Privatsphäre**.
  Klicken Sie in der Bitdefender VPN-Kachel auf **Öffnen**.
- Klicken Sie in der Menüleiste auf das -Symbol.
- Rufen Sie den Ordner Programme auf, öffnen Sie den Ordner Bitdefender und doppelklicken Sie dann auf das Bitdefender VPN-Symbol.

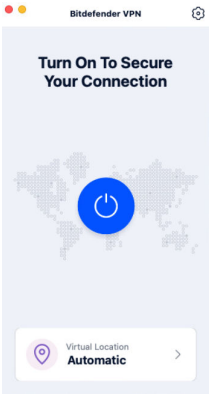
Beim ersten Öffnen der App werden Sie aufgefordert, Bitdefender das Hinzufügen von Konfigurationen zu erlauben. Indem Sie Bitdefender erlauben, Konfigurationen hinzuzufügen, stimmen Sie zu, dass alle Netzwerkaktivitäten Ihres Geräts gefiltert oder überwacht werden können, wenn Sie die VPN-App verwenden.

> **Hinweis**
> Die Bitdefender VPN-App kann nur auf macOS Sierra (10.12.6), macOS High Sierra (10.13.6) oder macOS Mojave (10.14) oder späteren Versionen des Betriebssystems installiert werden.

5.3. Oberfläche

In der VPN-Benutzeroberfläche wird der Status der App angezeigt, verbunden oder getrennt. Der Serverstandort wird für Anwender mit der kostenlosen Version von Bitdefender automatisch auf den geeignetsten Server festgelegt. Premium-Anwender können den Serverstandort selbst wählen, indem sie ihn aus der Liste Virtueller Standort auswählen. Weitere Einzelheiten zu den VPN-Abonnments finden Sie unter Abonnements (Seite 37).

Klicken Sie auf die Statusanzeige oben, um die Verbindung herzustellen oder zu trennen. Ein schwarzes Symbol in der Menüleiste zeigt an, dass eine Verbindung besteht. Ist das Symbol weiß, wurde die Verbindung getrennt.



Während die Verbindung besteht, wird die verstrichene Zeit unten in der Benutzeroberfläche angezeigt. Klicken Sie oben rechts auf das ⚙-Symbol, um auf weitere Optionen zuzugreifen.

- **Mein Konto** - Hier finden SIe Einzelheiten zu Ihrem Bitdefender-Benutzerkonto und Ihrem VPN-Abonnement. Klicken Sie auf **Konto wechseln**, wenn Sie sich mit einem anderen Konto anmelden möchten.
- **Einstellungen** - Hier können Sie das Produktverhalten individuell anpassen:
  - **Allgemein**
    - Benachrichtigungen - Sehen Sie sich Produktbenachrichtigungen an.
    - Beim Start ausführen - Bitdefender VPN wird automatisch bei Anmeldung gestartet.
    - Produktberichte - Übermitteln Sie anonyme Produktberichte, damit wir für Sie Benutzerfreundlichkeit und Schutzwirkung verbessern können.
  - **Erweitert**
    - Internet-Not-Aus - Unterbricht vorübergehend den Internetverkehr, wenn die Verbindung zum VPN-Server abbricht.
    - Werbeblocker und Anti-Tracker - Blockieren Sie Werbung und Tracker für ein aufgeräumtes und schnelleres Interneterlebnis.
    - Split-Tunneling - Die ausgewählten Websites umgehen das VPN und greifen direkt auf das Internet zu.

> **Hinweis**
> Klicken Sie auf **Verwalten** und dann **Webseite hinzufügen**, um dieser Liste Webseiten hinzuzufügen.

- Autom. Verbindung - VPN-Verbindung automatisch herstellen, wenn:
  - Verbindungen, die mit ungesicherten oder öffentlichen WLANs hergestellt werden.
  - Peer-to-Peer-File-Sharing-Anwendungen gestartet werden.

- **Support** - Sie werden auf die Support Center-Platform weitergeleitet. Hier finden Sie einen hilfreichen Artikel zur richtigen Nutzung von Bitdefender VPN.
- **Über** - Hier finden Sie Informationen über die installierte Version.
- **Beenden** - Beendet die App.

5.4. Abonnements

Mit Bitdefender VPN erhalten Sie ein kostenloses Datenvolumen von 200 MB pro Tag, um Verbindungen bei Bedarf abzusichern. Sie werden automatisch mit dem für Sie optimalen Serverstandort verbunden.

Wenn Sie sich für ein Upgrade auf die Premium-Version entscheiden, entfällt das Datenlimit und Sie können durch die freie Wahl des Serverstandorts Inhaltsbeschränkungen überall auf der Welt umgehen.

Mit einem Klick auf **Upgrade** können Sie über die Benutzeroberfläche jederzeit ein Upgrade auf Bitdefender Premium VPN durchführen.

Das Bitdefender Premium VPN-Abonnement ist nicht an das Bitdefender Antivirus for Mac-Abonnement gebunden, d. h. Sie können es während der gesamten Laufzeit nutzen, unabhängig vom Status Ihres Sicherheitsabonnements. Falls das Bitdefender Premium VPN-Abonnement ausläuft, aber das Abonnement für Bitdefender Antivirus for Mac weiterhin aktiv ist, werden Sie wieder auf die kostenlose Version umgestellt.

Bitdefender VPN ist plattformunabhängig und in den Windows-, macOS-, Android- und iOS-Produkten von Bitdefender verfügbar. Nach einem Premium-Upgrade können Sie Ihr Abonnement in allen Produkten nutzen,

vorausgesetzt, dass Sie sich mit dem gleichen Bitdefender-Benutzerkonto anmelden.

6. PRÄFERENZEN KONFIGURIEREN

Dieses Kapitel enthält die folgenden Themen:

6.1. Zugriff auf Präferenzen

Um das Präferenzen-Fenster von Bitdefender Antivirus for Mac zu öffnen:

- Wählen Sie eine der folgenden Methoden:
  - Klicken **Einstellungen** im Navigationsmenü der Bitdefender-Benutzeroberfläche.
  - Klicken Sie in der Menüleiste auf Bitdefender Antivirus for Mac und wählen Sie **Präferenzen**.

6.2. Schutzeinstellungen

Über das Schutzeinstellungsfenster können Sie den gesamten Scan-Vorgang konfigurieren. Sie können die Aktionen, die bei infizierten oder verdächtigen Dateien vorgenommen werden sollen oder auch allgemeine Einstellungen konfigurieren.

- **Bitdefender Shield.** Bitdefender Shield bietet Echtzeitschutz vor einer Vielzahl von Bedrohungen, indem es alle installierten Anwendungen, ihre aktualisierten Versionen sowie neue und geänderte Dateien scannt. Wir raten davon ab, Bitdefender Shield zu deaktivieren. Wenn Sie es dennoch deaktivieren müssen, sollten Sie dies nicht länger als absolut notwendig tun. Wenn Bitdefender Shield deaktiviert ist, sind Sie nicht vor Bedrohungen geschützt.
- **Nur neue und veränderte Dateien scannen.** Aktivieren Sie dieses Kästchen, wenn Bitdefender Antivirus for Mac nur Dateien prüfen soll, die vorher noch nicht geprüft wurden oder seit dem letzten Scan verändert wurden.

Sie können festlegen, dass diese Einstellung für benutzerdefinierte und Drag-&-Drop-Scans nicht angewandt wird, indem Sie das entsprechende Kästchen deaktivieren.

- **Backup-Inhalte nicht scannen.** Aktivieren Sie dieses Kästchen, um Backup-Dateien vom Scan auszuschließen. Wenn infizierte Dateien zu einem späteren Zeitpunkt wiederhergestellt werden, wird Bitdefender Antivirus for Mac sie automatisch erkennen und die entsprechenden Maßnahmen ergreifen.

6.3. Erweiterte Einstellungen

Sie können eine übergeordnete Aktion auswählen, die für alle Probleme und verdächtige Objekte, die während eines Scan-Vorgangs gefunden werden, durchgeführt werden soll.

Vorgehen bei infizierten Objekten

- **Versuchen, zu desinfizieren oder in die Quarantäne zu verschieben** - Wenn infizierte Dateien gefunden werden, versucht Bitdefender, sie zu desinfizieren (den Schadcode zu entfernen) oder sie in die Quarantäne zu verschieben.
- **Keine Aktion durchführen** - Es werden keine Aktionen für die gefundenen Dateien durchgeführt.

Vorgehen bei verdächtigen Objekten

- **Dateien in Quarantäne verschieben** - Wenn verdächtige Dateien gefunden werden, verschiebt Bitdefender sie in die Quarantäne.
- **Keine Aktion durchführen** - Für die erkannten Dateien wird keine Aktion ausgeführt.

6.4. Sonderangebote

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 der Bitdefender-Benutzeroberfläche.

2. Wechseln Sie zum Reiter **Sonstige**.
3. Aktivieren oder deaktivieren Sie den Schalter **Meine Angebote**.

> **Hinweis**
> Die Option **Meine Angebote** ist standardmäßig aktiviert.

7. 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 verbunden 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:
  - Bitdefender Antivirus for Mac
  - Die Bitdefender-Produktlinie für Windows
  - Bitdefender Mobile Security for Android
  - Bitdefender Mobile Security for iOS
- Verwaltung und Verlängerung Ihrer Bitdefender-Abonnements.
- Neue Geräte zu Ihrem Netzwerk hinzufügen und per Fernzugriff verwalten.

7.1. Aufrufen von Bitdefender Central

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

- Über das Bitdefender Antivirus for Mac-Hauptfenster:
  1. Klicken Sie rechts unten in der Benutzeroberfläche auf den Link **Zum eigenen Konto**.
- Über Ihren Web-Browser:
  1. Öffnen Sie einen Web-Browser auf jedem beliebigen internetfähigen Gerät.
  2. Gehe 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.

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

7.2. Zwei-Faktor-Authentifzierung

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.

7.2.1. 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. Rufen Sie **Bitdefender Central** auf.

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. 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 Authentifizierungsanwendung verwenden möchten, sich aber nicht sicher sind, welche App Sie verwenden sollen, können Sie sie aus einer Liste mit von uns empfohlenen Authentifizierungsanwendungen auswählen.

     a. Klicken Sie zunächst auf **AUTHENTIFIZIERUNGSANWENDUNG VERWENDEN**.

     b. Scannen Sie Anmeldung auf einem Android- oder iOS-Gerät den QR-Code mit dem Gerät.
     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**.

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 Authentifizierungscodes 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.

7.3. 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 Central.
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.

7.4. Meine Geräte

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

7.4.1. Hinzufügen eines neuen Geräts

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

7.4.2. 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 **Gerätename** 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**.

7.4.3. 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 Probleme 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 erneuen 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.

7.5. 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.

7.6. Meine Abonnements

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

7.6.1. 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.

7.6.2. 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.

7.6.3. 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.

7.7. 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.

8. HÄUFIG GESTELLTE FRAGEN

Wie kann ich Bitdefender Antivirus for Mac testen, bevor ich mich für ein Abonnement entscheide?

Sie sind ein neuer Bitdefender-Kunde und möchten unser Produkt testen, bevor Sie es kaufen. Der Testzeitraum beträgt 30 Tage. Nach Ablauf dieser Frist können Sie das Produkt nur weiterverwenden, wenn Sie ein Bitdefender-Abonnement erwerben. So erhalten Sie die Bitdefender Antivirus for Mac-Testversion:

1. Erstellen Sie ein Bitdefender-Konto wie folgt:
   a. Gehe zu: https://central.bitdefender.com.
   b. Geben Sie die Daten in die entsprechenden Felder ein. Die hier eingetragenen Daten werden vertraulich behandelt.
   c. 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.
   d. Klicken Sie auf **BENUTZERKONTO ERSTELLEN**.

2. Laden Sie Bitdefender Antivirus for Mac wie folgt herunter:
   a. Wähle aus **Meine Geräte** Panel, und klicken Sie dann auf **SCHUTZ INSTALLIEREN**.
   b. Wählen Sie eine der beiden verfügbaren Optionen:
      - **Schützen Sie dieses Gerät**
        i. Wählen Sie diese Option und dann den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, klicken Sie auf die entsprechende Schaltfläche.
        ii. Speichern Sie die Installationsdatei.
      - **Schützen Sie andere Geräte**

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

ii. Klicken **DOWNLOADLINK SENDEN**.

iii. 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.

iv. 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.

c. Führen Sie das heruntergeladene Bitdefender-Produkt aus.

Ich habe einen Aktivierungscode. Wie verlängere ich damit die Laufzeit meines Abonnements?

Wenn Sie einen Aktivierungscode von einem unserer Reseller erworben oder geschenkt bekommen haben, können Sie die Verfügbarkeit zu Ihrem Bitdefender-Abonnement hinzufügen.

Gehen Sie folgendermaßen vor, um ein Abonnement mit einem Aktivierungscode zu aktivieren:

1. Zugang Bitdefender Central.
2. Wähle aus **Meine Abonnements** Tafel.
3. Drücke den **AKTIVIERUNGSCODE** Schaltfläche und geben Sie dann den Code in das entsprechende Feld ein.
4. Klicken **AKTIVIEREN SIE** weitermachen.

Die Erweiterung wird jetzt in Ihrem Bitdefender-Konto sowie im rechten unteren Bereich der Oberfläche Ihres installierten Bitdefender Antivirus for Mac-Produkts angezeigt.

Das Scan-Protokoll zeigt noch nicht gelöste Probleme an. Wie kann ich diese beheben?

Mögliche noch nicht gelöste Probleme im Scan-Protokoll sind zum Beispiel:

- Archive mit eingeschränktem Zugriff (xar, rar usw.)
  Lösung: Lokalisieren Sie die Datei über die Option **Im Finder anzeigen** und löschen Sie sie von Hand. Vergessen Sie dabei nicht, den Papierkorb zu leeren.
- Postfächer mit eingeschränktem Zugriff (Thunderbird usw.)
  Lösung: Entfernen Sie den Eintrag mit der infizierten Datei mithilfe der Anwendung.
- Backup-Inhalte
  Lösung: Aktivieren Sie in den Schutz-Einstellungen die Option **Backup-Inhalte nicht scannen** oder schließen Sie die gefundenen Dateien mit **Zu den Ausnahmen hinzufügen** vom Scan aus.
  Werden infizierte Dateien zu einem späteren Zeitpunkt wiederhergestellt, erkennt Bitdefender Antivirus for Mac diese automatisch und leitet geeignete Maßnahmen ein.

> **Hinweis**
> Dateien mit beschränktem Zugriff sind Dateien, die Bitdefender Antivirus for Mac zwar öffnen, aber nicht bearbeiten kann.

Wo kann ich detaillierte Informationen zu den Produktaktivitäten einsehen?

Bitdefender führt ein Protokoll über alle wichtigen Aktionen, Statusänderungen und andere kritische Nachrichten über die eigenen Aktivitäten. Um auf diese Informationen zuzugreifen, klicken Sie im Navigationsmenü der Bitdefender-Oberfläche auf **Benachrichtigungen**.

Kann ich Bitdefender Antivirus for Mac über einen Proxy-Server aktualisieren?

Bitdefender Antivirus for Mac kann nur über Proxy-Server aktualisieren, die keine Authentifizierung erfordern. Sie müssen keine Programmeinstellungen konfigurieren.

Wenn Sie sich über einen Proxyserver mit dem Internet verbinden, der eine Authentifizierung erfordert, müssen Sie regelmäßig zu einer direkten Internetverbindung wechseln, um Aktualisierungen der Bedrohungsinformationen zu erhalten.

Wie kann ich Bitdefender Antivirus for Mac entfernen?

Gehen Sie folgendermaßen vor, um Bitdefender Antivirus for Mac zu entfernen:

1. Öffnen Sie **Finder** und wählen Sie den Programme-Ordner.
2. Öffnen Sie den Bitdefender-Ordner und doppelklicken Sie auf BitdefenderUninstaller.
3. Klicken **Deinstallieren** und warten Sie, bis der Vorgang abgeschlossen ist.
4. Klicken **Schließen** beenden.

> **Wichtig**
> Wenn ein Fehler auftritt, können Sie sich wie in beschrieben an den Bitdefender-Kundendienst wenden Hier wird Ihnen geholfen (Seite 58).

Wie entferne ich die Linkchecker-Erweiterungen aus meinem Browser?

- So können Sie die TrafficLight-Erweiterungen aus Mozilla Firefox entfernen:
  1. Gehen Sie zu **Tools** und wählen Sie **Add-ons**.
  2. Klicken Sie in der Spalte links auf **Erweiterungen**.
  3. Wählen Sie die Erweiterung aus und klicken Sie auf **Entfernen**.
  4. Starten Sie den Browser neu, um den Entfernungsvorgang abzuschließen.
- So können Sie die TrafficLight-Erweiterung aus Google Chrome entfernen:
  1. Klicken Sie oben rechts auf **Mehr** ⋮.
  2. Gehen Sie zu **Weitere Tools** und wählen Sie **Erweiterungen**.
  3. Klicken Sie auf das **Entfernen** 🗑-Symbol neben der Erweiterung, die Sie entfernen möchten.
  4. Klicken Sie auf **Entfernen**, um den Entfernungsvorgang zu bestätigen.
- So können Sie Bitdefender TrafficLight aus Safari entfernen:

1. Rufen Sie die **Einstellungen** auf oder nutzen Sie die Tastenkombination **Befehl-Komma(,)**.
2. Wählen Sie **Erweiterungen**.
   Eine Liste mit allen installierten Erweiterungen wird angezeigt.
3. Wählen Sie die Bitdefender TrafficLight-Erweiterung aus und klicken Sie auf **Deinstallieren**.
4. Klicken Sie erneut auf **Deinstallieren**, um den Deinstallationsvorgang zu bestätigen.

Wann sollte ich Bitdefender VPN verwenden?

Bei Aufrufen, Herunterladen oder Hochladen von Inhalten im Internet sollten Sie stets Vorsicht walten lassen. Um sicherzustellen, dass Sie beim Surfen im Netz jederzeit geschützt sind, empfehlen wie den Einsatz von Bitdefender VPN, wenn Sie:

- Verbindungen zu öffentlichen WLAN-Netzwerken herstellen möchten
- auf Inhalte zugreifen möchten, die regionalen Zugangsbeschränkungen unterliegen, egal ob Sie zuhause oder im Ausland sind
- Ihre persönlichen Daten vor Zugriff schützen möchten (Benutzernamen, Passwörter, Kreditkartendaten etc.)
- Ihre IP-Adresse verbergen möchten

Wirkt sich Bitdefender VPN auf die Akkulaufzeit meines Gerätes aus?

Bitdefender VPN wurde entwickelt, um Ihre persönlichen Daten zu schützen, Ihre IP-Adresse bei Verbindungen mit ungesicherten WLAN-Netzwerken zu verbergen und Ihnen den Zugriff auf Inhalte mit länderspezifischen Zugangsbeschränkungen zu ermöglichen. Um Ihren Akku zu entlasten, empfehlen wir, das VPN nur bei Bedarf zu nutzen und die Verbindung danach wieder zu trennen.

Warum wird meine Internetverbindung langsamer, wenn ich eine Verbindung mit Bitdefender VPN herstelle?

Bitdefender VPN ist auf einen ressourcenschonenden Betrieb beim Surfen im Netz ausgelegt. Ihre Internetverbindung bzw. die Entfernung zum Server, mit dem Sie eine Verbindung hergestellt haben, können sich jedoch negativ auf die Verbindungsgeschwindigkeit auswirken. Wenn es nicht unbedingt notwendig ist, dass Sie sich von Ihrem

Standort aus mit einem weit entfernten Server verbinden (z. B. von Deutschland aus nach China), sollten Sie in solchen Fällen Bitdefender VPN erlauben, automatisch eine Verbindung mit dem nächstgelegenen Server herzustellen bzw. einen Server zu finden, der näher an Ihrem Standort liegt.

9. HILFE UND SUPPORT

9.1. 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.

9.2. 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 Lieblingssuchmaschine.

9.2.1. 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 berechtigen Informationsanfragen oder Fehlermeldungen von Bitdefender-Kunden finden sich über kurz oder lang im Bitdefender Support Center wieder und dienen als Bugfix-Anleitungen, Umgehungslösungen oder Informationsartikel, die die Hilfedateien des Produkts ergänzen sollen.

Das Bitdefender Support Center ist jederzeit unter der folgenden Adresse erreichbar: https://www.bitdefender.de/consumer/support/.

9.2.2. 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

9.2.3. 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.

9.3. 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/

9.3.1. 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 AktiveX die Sicherheitskontrollen fehlen, deshalb raten Computersicherheitsexperten davon ab, AktiveX 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, der den Bootsektor einer Festplatte oder eines Diskettenlaufwerks infiziert. Beim Versuch von einer Diskette, die mit einem Bootvirus infiziert ist, zu booten wird diese Bedrohung im Arbeitsspeicher aktiviert. Bei jedem Neustart wird die Bedrohung so im Arbeitsspeicher aktiviert und überträgt sich auf eingelegte Wechselmedien.

Botnet

Der Begriff "Botnet" setzt sich aus den Wörtern "Robot" und "Network" zusammen. Bei Botnets handelt es sich um ein Netz aus mit Bedrohungen infizierten Geräten, die mit dem Internet verbunden und für den Versand von Spam, den Diebstahl von Daten, die Fernsteuerung von anfälligen Geräten oder die Verbreitung von Spyware, Ransomware und anderen

Bedrohungsarten verwendet werden. Ziel ist es, möglichst viele mit dem Internet verbundene Geräte zu infizieren, so z. B. PCs, Server, Mobilgeräte oder IoT-Geräte in den Netzwerken großer Unternehmen oder Branchen.

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. Anderseits bedeutet es, dass Online-Aktivitäten der Benutzer gewissermaßen auf Schritt und "Klick" verfolgt werden. Es ist also verständlich, dass in diesem Zusammenhang

Datenschutz ein umstrittenes Thema ist und viele sich unwohl fühlen, quasi als SKU-Nummer (die Strichcodes auf den Packungen, die im Geschäft an der Theke gescannt werden) betrachtet zu werden. Auch wenn diese Sicht etwas extrem erscheint, ist sie doch manchmal korrekt.

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 Virenscanner 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 eine Spam-Nachricht, das Herunterladen eines E-Mail-Anhangs oder die Installation von Anwendungen ausbreiten, ohne dass der Benutzer es überhaupt bemerkt. Ransomware-Hacker nehmen herkömmliche Benutzer und Unternehmen ins Visier.

Berichtsdatei

Eine Datei, die stattgefundene Aktivitäten aufzeichnet.Zum Beispiel speichert BitDefender eine Logdatei mit die 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.