Bitdefender

VPN

BENUTZERHANDBUCH

Bitdefender VPN

Benutzerhandbuch

Veröffentlichungsdatum: 21.11.2022

Rechtlicher Hinweis

Bitdefender

Inhaltsverzeichnis

ÜBER DIESE ANLEITUNG

Zielsetzung und Zielgruppe

Dieses Handbuch richtet sich an alle Bitdefender-Benutzer, die sich für Bitdefender VPN als ihren bevorzugten Dienst entschieden haben, um ihre Online-Anonymität durch Verschlüsselung des gesamten ein- und ausgehenden Datenverkehrs auf ihrem PC, Mac oder Mobilgeräten zu gewährleisten.

Hier erfahren Sie, wie Sie Bitdefender VPN konfigurieren und einsetzen, um Ihre Online-Identität und -Aktivitäten vor Hackern, Internetdienstleistern und Datenschnüfflern zu schützen, und wie Sie das Optimum aus Bitdefender herausholen.

Viel Spaß mit diesen nützlichen und informativen Handbuch.

Über dieses Handbuch

Dieses Handbuch behandelt die folgenden Themengebiete:

Was ist Bitdefender VPN (Seite 4)

Machen Sie Ihre ersten Schritte mit Bitdefender VPN, indem Sie erfahren, was genau es ist und wie es Ihnen durch Gewährleistung echter Online-Anonymität helfen kann, sich besser zu schützen.

Bitdefender VPN richtig nutzen (Seite 15)

Erfahren Sie mehr über den Umgang mit Bitdefender VPN und seiner Benutzeroberfläche.

Einstellungen & Funktionen von Bitdefender VPN (Seite 20)

Erfahren Sie mehr über die Einstellungen und den Funktionsumfang von Bitdefender VPN.

Hilfe und Support (Seite 32)

Hinweise zu nützlichen Informationen und Hilfestellungen bei unerwarteten Problemen.

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 VPN

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 Militärstandard verschlüsselt und Ihre IP-Adresse bleibt jederzeit unsichtbar. Ihr Datenverkehr wird über einen speziellen Server weitergeleitet, was es Ihrem Provider 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 einigen Ländern wird das Internet zensiert, weshalb der Einsatz von VPN dort gesetzlich nicht erlaubt ist. Um rechtliche Folgen vorzubeugen, kann es sein, dass eine Warnmeldung angezeigt wird, wenn Sie zum ersten Mal versuchen, die Funktion von Bitdefender VPN zu verwenden. Wenn Sie die Funktion dann verwenden, bestätigen Sie damit, dass Sie die relevanten Bestimmungen Ihres Landes kennen und sich der entsprechenden Risiken bewusst sind.

1.1. Verschlüsselungsprotokolle

Die Standard-Cipher-Suiten, die im Hydra-Client und -Server aktiviert sind, sind unten angegeben. Alle anderen Cipher-Suiten sind deaktiviert.

Hydra-Client-Cipher-Suites:

- ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA:AES128-SHA:AES256-SHA:DES-CBC3-SHA

Hinweis

Das serverseitige Set ist deutlich restriktiver; sowohl der Hydra-Client als auch der -Server lehnen alle Modi außer GCM mit AES ab. Der Hydra-Server erfordert serverseitige Priorität stärkerer Ciper-Suiten und lehnt TLS-Handshakes ab, wenn eine schwächere Suite von einem Client angefordert wird. Diese Liste ist während der Laufzeit auf der Server-Seite konfigurierbar.

2. VPN-ABONNEMENTS

Bei Bitdefender VPN haben Sie die Wahl zwischen zwei verschiedenen Abonnements:

- Das Basic-Abonnement
- Das Premium-Abonnement

2.1. Basic-Abonnement

Mit Bitdefender VPN steht Ihnen pro Gerät täglich ein Datenverkehrsvolumen von 200 MB kostenlos zur Verfügung. Die Verbindungen werden dabei immer zu einer nicht veränderbaren Adresse hergestellt.

Das Basic-Abonnement steht jedem zur Verfügung, der Bitdefender VPN herunterlädt.

2.2. Premium-Abonnement

Zugriff auf den vollen Funktionsumfang von Bitdefender VPN erhalten Sie mit einem Upgrade auf die Premium-Version. Mit einem Premium-VPN-Abonnement erhalten Sie unbeschränkten abgesicherten Datenverkehr und können die Verbindung über einen beliebigen unserer weltweit stationierten Server laufen lassen.

Das Premium-Abonnement gibt es in zwei verschiedenen Varianten: monatliches oder jährliches Abonnement.

- Mit dem monatlichen Abonnement erhalten Sie monatlich eine Rechnung über die Premium-Abonemment-Gebühr. Sie können jederzeit kündigen.
- Mit dem jährlichen Abonnement erhalten Sie einmal jährlich eine Rechnung über die Permium-Abonnement-Gebühr.

2.3. Upgrade auf Premium VPN

Wenn Sie ein Upgrade Ihres Bitdefender VPN-Abonnements auf die Premium-Version durchführen möchten, klicken Sie am einfachsten im unteren Bereich der Programmoberfläche auf die Schaltfläche **Upgrade**. Wählen Sie dann die gewünschte Abonnement-Variante und folgen Sie den angezeigten Anweisungen.

Wenn Sie bereits einen Aktivierungscode haben, gehen Sie wie folgt vor:

- **Für Windows-Benutzer**
  1. Klicken Sie links in der VPN-Oberfläche auf das Symbol für Ihr Konto.
  2. Klicken Sie auf **Hier hinzufügen**.
  3. Geben Sie den Code ein, den Sie per E-Mail erhalten haben, und klicken Sie dann auf **Code aktivieren**.
- **Für macOS-Benutzer**
  1. Klicken Sie rechts oben in der VPN-Oberfläche auf das Zahnrad und wählen Sie dann **Mein Konto**.
  2. Klicken **Fügen Sie es hier hinzu**.
  3. Geben Sie den per E-Mail erhaltenen Code ein und klicken Sie dann auf **Aktiviere Code** Taste.
- **Für Android-Benutzer**
  1. Tippen Sie rechts oben in der VPN-Oberfläche auf das Zahnrad und wählen Sie dann **Mein Konto**.
  2. Tippen Sie auf **Code hinzufügen**.
  3. Geben Sie den per E-Mail erhaltenen Code ein und klicken Sie dann auf **Aktiviere Code** Taste.
- **Für iOS-Benutzer**
  1. Tippen Sie auf das Zahnrad in der oberen rechten Ecke der VPN-Oberfläche und wählen Sie es aus **Mein Konto**.
  2. Klopfen **Code hinzufügen**.
  3. Geben Sie den per E-Mail erhaltenen Code ein und klicken Sie dann auf **Aktiviere Code** Taste.

3. DAS BITDEFENDER CENTRAL-KONTO

Zur Nutzung von Bitdefender VPN benötigen Sie ein aktives Bitdefender Central-Konto. Bitdefender Central ist der Name der Plattform, über die Sie Zugriff auf die Online-Funktionen und -Dienste des Produkts erhalten.

Über dieses Konto können Sie die folgenden Dinge tun:

- Laden Sie Bitdefender VPN herunter und installieren Sie es auf Windows-, macOS-, iOS- und Android-Betriebssystemen.
- Verwaltung und Verlängerung Ihrer Bitdefender-Abonnements.

3.1. Aufrufen von Bitdefender Central

So greifen sie auf Bitdefender Central zu:

- **Für Windows-Benutzer**
  1. Klicken Sie auf das Symbol Mein Konto auf der linken Seite der VPN-Oberfläche.
  2. Klicken Sie auf **Profil bearbeiten**.
- **Für macOS-Benutzer**
  1. Klicken Sie auf das Symbol Mein Konto auf der linken Seite der VPN-Oberfläche.
  2. Klicken **Profil bearbeiten**.
- **Für Android-Benutzer**
  1. Tippen Sie auf das Zahnrad in der oberen rechten Ecke der VPN-Oberfläche und wählen Sie es aus **Mein Konto**.
  2. Tippen Sie auf **Kontoinformationen in Bitdefender Central bearbeiten**.
- **Für iOS-Benutzer**
  1. Tippen Sie auf das Zahnrad in der oberen rechten Ecke der VPN-Oberfläche und wählen Sie es aus **Mein Konto**.
  2. 2. Tippen Sie auf **Kontoinformationen in Bitdefender Central bearbeiten**.

Alternativ können Sie Ihr Bitdefender Central-Konto auch über https://central.bitdefender.com aufrufen.

4. INSTALLATION

4.1. Vor der Installation

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

- Stellen Sie sicher, dass das Zielgerät für die Bitdefender-Installation die Systemvoraussetzungen erfüllt. Wenn das Gerät die Systemvoraussetzungen nicht erfüllt, kann Bitdefender nicht installiert werden. Falls es doch installiert wird, kann es zu Leistungseinbußen und Stabilitätsproblemen kommen.
  Eine vollständige Liste der Systemanforderungen finden Sie unter Systemanforderungen (Seite 10).
- Melden Sie sich mit einem Administrator-Konto am Gerät an.
- Ihr Gerät sollte während der Installation mit dem Internet verbunden sein, auch wenn Sie von CD oder DVD installieren. Falls neuere Versionen der Anwendungsdateien aus dem Installationspaket verfügbar sind, kann Bitdefender diese dann herunterladen und installieren.

4.2. Systemanforderungen

- **Für Windows-Benutzer**
  - **Betriebssystem:** Windows 7 mit Service Pack 1, Windows 8, Windows 8.1 und Windows 10
  - **Speicher (RAM):** 1 GB
  - **Verfügbarer freier Festplattenspeicher:** 500 MB freier Speicher
  - **.NET Framework:** Mindestversion 4.5.2

    Wichtig
    Die Systemleistung kann auf Geräten mit CPUs der alten Generation beeinträchtigt werden.
- **Für macOS-Benutzer**
  - **Betriebssystem:** macOS Sierra (10.12) und höher

- **Verfügbarer freier Festplattenspeicher:** 100 MB freier Speicher

- **Für Android-Benutzer**
  - **Betriebssystem:** Android 5.0 oder höher
  - **Speicher:** 100 MB
  - Eine aktive Internet-Verbindung

- **Für iOS-Benutzer**
  - **Betriebssystem:** iOS 12 und höher
  - **Speicher auf iPhone:** 50 MB
  - **Speicher auf iPad:** 100 MB
  - Eine aktive Internetverbindung

4.3. Bitdefender VPN wird installiert

Folgen Sie den Installationsanweisungen für Ihr Betriebssystem:

- **Für Windows-Benutzer**

  1. Um Bitdefender VPN auf einem Windows-PC zu installieren, laden Sie einfach das Installationspaket von https://www.bitdefender.com/solutions/vpn/download herunter. Alternativ können Sie den Download auch über die E-Mail starten, die Sie nach dem Kauf erhalten haben.
  2. Doppelklicken Sie auf das heruntergeladene Installationsprogramm, um es auszuführen.
  3. Wenn das Dialogfenster der Benutzerkontensteuerung angezeigt wird, klicken Sie auf Ja.
  4. Warten Sie, bis der Download abgeschlossen ist.
  5. Wählen Sie über das Klappmenü im Installer die Sprache, in der die Software installiert werden soll.
  6. Markieren Sie das Kästchen neben „Hiermit bestätige ich, dass ich die Nutzungsbedingungen und die Datenschutzerklärung gelesen habe und sie akzeptiere“ und klicken Sie dann auf **INSTALLATION STARTEN**.

7. Warten Sie, bis der Installationsvorgang abgeschlossen ist.
8. Jetzt können Sie sich mit Ihrem Bitdefender Central-Konto **ANMELDEN**. Wenn Sie noch kein Central-Konto haben, können Sie über die Schaltfläche **KONTO ERSTELLEN** ein neues Konto erstellen.
9. Wählen Sie **Ich habe einen Aktivierungscode**, wenn Sie bereits einen Premium VPN-Abonnement erworben haben.
   Alternativ können Sie auf **TESTPHASE BEGINNEN** klicken und damit die Software 7 Tage lang kostenlos testen, bevor Sie eine Kaufentscheidung treffen.
10. Geben Sie den Code ein, den Sie per E-Mail erhalten haben, und klicken Sie dann auf **PREMIUM AKTIVIEREN**.
11. Nach kurzer Wartezeit ist Bitdefender VPN installiert und Sie können es auf Ihrem Computer nutzen.

- **Für macOS-Benutzer**

1. Um Bitdefender VPN auf macOS zu installieren, laden Sie einfach das Installationspaket von https://www.bitdefender.com/solutions/vpn/download herunter. Alternativ können Sie den Download auch über die E-Mail starten, die Sie nach dem Kauf erhalten haben.
2. Der Installer wird auf Ihrem Mac gespeichert. Doppelklicken Sie auf die -Paket-Datei im Downloads-Ordner.
3. Folgen Sie den angezeigten Anweisungen. Klicken Sie dann auf **Fortfahren**.
4. Sie werden Schritt für Schritt durch die Installation von Bitdefender VPN auf Ihrem Mac geleitet. Klicken Sie zweimal auf **Fortfahren**.
5. Klicken Sie, wenn Sie die Lizenzvereinbarung gelesen haben und sie akzeptieren, auf **Zustimmen**.
6. Klicken Sie auf **Installieren**.
7. Geben Sie den Benutzernamen und das Kennwort eines Administrators ein und klicken Sie danach auf **Software installieren**.
8. Sie erhalten eine Meldung, dass eine von Bitdefender signierte Systemerweiterung blockiert wurde. Dabei handelt es sich nicht

um einen Fehler, sondern nur um eine Sicherheitsmaßnahme. Klicken Sie auf **Sicherheitseinstellungen öffnen**.

9. Klicken Sie auf das Schlosssymbol, um die Sperre aufzuheben.
   Geben Sie Namen und Passwort eines Administrators ein und klicken Sie dann auf **Freischalten**.
10. Klicken Sie auf **Zulassen**, um die Systemerweiterung für Bitdefender Bitdefender zu laden. Schließen Sie dann das Fenster Sicherheit und Datenschutz und das Bitdefender-Installationsprogramm.
11. Klicken Sie auf das Schildsymbol in der Menüleiste und **melden Sich sich** an Ihrem Bitdefender-Central-Konto an. Wenn Sie noch keines haben, erstellen Sie bitte eines.
12. Wählen Sie **Ich habe einen Aktivierungscode**, wenn Sie bereits einen Premium-VPN-Abonnement erworben haben.
    Ansonsten können Sie wählen **TESTVERSION STARTEN** um das Produkt 7 Tage lang kostenlos zu testen, bevor Sie sich zur Zahlung verpflichten.
13. Geben Sie den per E-Mail erhaltenen Code ein und klicken Sie dann auf **Aktiviere Code** Taste.
14. Nach kurzer Wartezeit ist Bitdefender VPN installiert und Sie können es auf Ihrem Mac nutzen.

- **Für Android-Benutzer**

1. Auf Android-Geräten installieren Sie Bitdefender VPN, indem Sie zunächst den **Google Play Store** auf Ihrem Smartphone oder Tablet öffnen.
2. Suchen Sie nach Bitdefender VPN und wählen Sie die entsprechende App aus.
3. Tippen Sie auf die Schaltfläche **Installieren** und warten Sie, bis der Download abgeschlossen ist.
4. Tippen Sie auf **Öffnen**, um die App zu starten.
5. Markieren Sie das Kästchen neben „Ich akzeptiere die Nutzungsbedingungen und Datenschutzerklärung“ und tippen Sie auf **Fortfahren**.

6. Jetzt können Sie sich mit Ihrem Bitdefender Central-Konto **Anmelden**. Wenn Sie noch kein Central-Konto haben, können Sie über die Schaltfläche **Konto erstellen** ein neues Konto erstellen.
7. Wählen Sie {1}Ich habe einen Aktivierungscode{2}, wenn Sie bereits einen Premium-VPN-Abonnement erworben haben.
   Alternativ können Sie auf „7-tägige Testphase starten“ klicken und damit die Software 7 Tage lang kostenlos testen, bevor Sie eine Kaufentscheidung treffen.
8. Geben Sie den Code ein, den Sie per E-Mail erhalten haben, und tippen Sie dann auf **Code aktivieren**.

- **Für iOS-Benutzer**

1. Öffnen Sie zur Installation von Bitdefender VPN unter iOS zunächst den **App Store** auf Ihrem iPhone oder iPad.
2. Suchen nach Bitdefender VPN und wählen Sie diese App aus.
3. Tippen Sie auf das Symbol **Herunterladen** und warten Sie, bis der Download abgeschlossen ist.
4. Klopfen **Offen** um die App auszuführen.
5. Markieren Sie das Kästchen neben **Ich akzeptiere die Nutzungsbedingungen und die Datenschutzerklärung** und tippen Sie auf **Fortfahren**.
6. Jetzt können Sie sich mit Ihrem Bitdefender Central-Konto **Anmelden**. Wenn Sie noch kein Konto haben, können Sie über die Schaltfläche **Konto erstellen** ein neues Konto erstellen.
7. Tippen Sie auf **Zulassen**, wenn Sie Benachrichtigungen von Bitdefender VPN erhalten möchten.
8. Wählen **Ich habe einen Aktivierungscode** wenn Sie ein Premium-VPN-Abonnement erworben haben.
   Andernfalls können Sie 7 Tage Testversion starten auswählen, um das Produkt 7 Tage lang kostenlos zu testen, bevor Sie sich zur Zahlung verpflichten.
9. Geben Sie den per E-Mail erhaltenen Code ein und tippen Sie dann auf **Aktiviere Code**.

5. BITDEFENDER VPN RICHTIG NUTZEN

5.1. Bitdefender VPN öffnen

- **Unter Windows**
  Es gibt verschiedene Möglichkeiten, das **Bitdefender VPN-Hauptfenster** zu öffnen:
  - **Über die Taskleiste**
    Rechtsklicken Sie auf das rote Schildsymbol in der Taskleiste und wählen Sie dann im Menü **Anzeigen**.
  - **Über die Bitdefender-Benutzeroberfläche**
    Wenn bereits ein Bitdefender-Sicherheitsprodukt wie z. B. Bitdefender Total Security oder Bitdefender Antivirus Plus auf Ihrem Windows-Computer installiert ist, können Sie Bitdefender VPN auch von dort aus öffnen:
    1. Klicken Sie links in der Bitdefender-Benutzeroberfläche auf **Privatsphäre**.
    2. Klicken Sie im VPN-Bereich auf **VPN öffnen**.
  - **Über Ihren Desktop**
    Doppelklicken Sie auf die Bitdefender VPN-Verknüpfung auf Ihrem Desktop.
- **Unter macOS**
  Sie können die Bitdefender VPN-App öffnen, indem Sie auf das Symbol in der Menüleiste oben rechts auf dem Bildschirm klicken.
  Wenn Sie das Bitdefender-Schild in der Menüleiste nicht finden können, verwenden Sie das Mac-Launchpad oder den Finder, um es wieder anzuzeigen:
  - **Über das Launchpad**
    1. Drücken Sie **F4** auf Ihrer Tastatur, um das Launchpad auf Ihrem Mac aufzurufen.
    2. Suchen Sie unter den installierten Apps nach der Bitdefender VPN-App oder geben Sie **Bitdefender VPN** im Launchpad ein, um die Ergebnisse zu filtern.

3. Wenn Sie die Bitdefender VPN-App gefunden haben, können Sie auf das entsprechende Symbol klicken, um sie an die Menüleiste anzuheften.

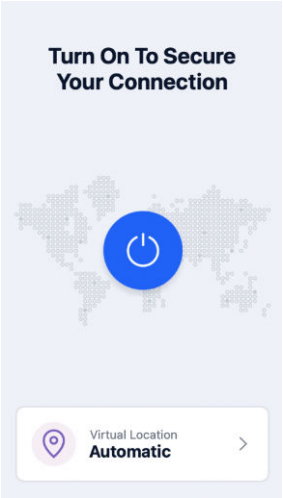
- **Über den Finder**

1. Klicken Sie unten links im Dock auf den **Finder** (das blaue Quadrat mit dem lächelnden Gesicht).
2. Klicken Sie danach auf **Los** in der Menüleiste oben links auf dem Bildschirm.
3. Wählen Sie im Menü die Option **Programme**, um den Ordner Programme auf Ihrem Mac aufzurufen.
4. Öffnen Sie im Ordner Programme den Ordner **Bitdefender** und doppelklicken Sie dann auf die **Bitdefender VPN**-App.

Hinweis
Um Bitdefender VPN auf Ihren Android- oder iOS-Mobilgeräten aufzurufen, müssen Sie Bitdefender VPN-App nach der Installation lediglich öffnen.

5.2. Verbindung mit Bitdefender VPN herstellen

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. Zum Herstellen bzw. Trennen der Verbindung müssen Sie in der VPN-Oberfläche lediglich auf die Einschalttaste klicken.



- **Unter Windows:** Das Symbol in der Taskleiste zeigt ein grünes Häkchen an, wenn das VPN verbunden ist. Ein schwarzes Häkchen zeigt an, dass keine VPN-Verbindung besteht. Wenn eine Verbindung zu einem manuell ausgewählten Standort besteht, wird die IP-Adresse im Hauptfenster angezeigt.
- **Unter macOS:** Das Symbol in der Menüleiste ist schwarz, wenn das VPN verbunden ist, und weiß, wenn die VPN-Verbindung getrennt ist. Klicken Sie auf die kreisförmige Schaltfläche in der Mitte der Benutzeroberfläche und warten Sie, bis die Verbindung hergestellt wird.
- **Unter Android & iOS:** So stellen Sie unter Android, iOS und iPadOS eine Bitdefender VPN-Verbindung her:
  - **In der Bitdefender VPN-App:** Zum Herstellen bzw. Trennen der Verbindung müssen Sie in der VPN-Oberfläche lediglich auf die Einschalttaste tippen. Der Status von Bitdefender VPN wird angezeigt.
  - **In der Bitdefender Mobile Security-App:**
    1. Rufen Sie das VPN-Symbol in der unteren Navigationsleiste von Bitdefender Mobile Security auf.

2. Tippen Sie auf **VERBINDEN**, um sich bei Verbindungen mit ungesicherten WLAN-Netzwerken zu schützen. Tippen Sie auf **TRENNEN**, wenn Sie die VPN-Verbindung deaktivieren möchten.

5.3. Verbindung mit einem anderen Server herstellen

Mit einem Premium-Abonnement können Sie mit Bitdefender VPN jederzeit eine Verbindung zu einem unserer Server in aller Welt herstellen. Gehen Sie dazu wie folgt vor:

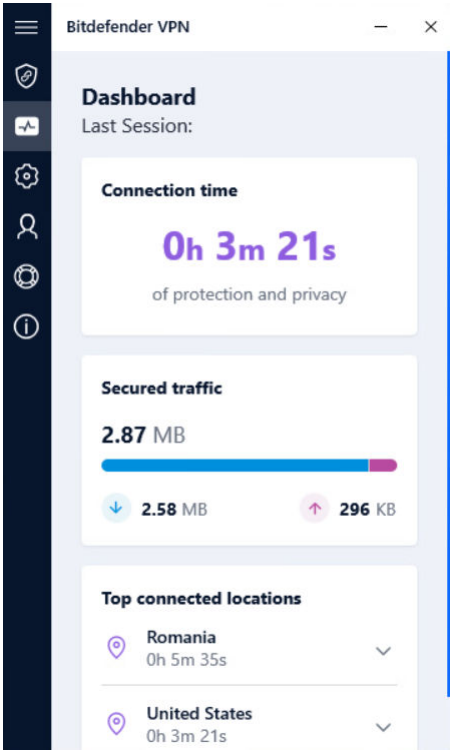
1. Öffnen Sie die Bitdefender VPN-App.
2. Tippen Sie im unteren Bereich der Programmoberfläche auf die Schaltfläche **Virtueller Standort**.
3. Wählen Sie ein beliebiges Land aus.
4. Klicken Sie unten auf die Schaltfläche **Verbindung nach [Land] aufbauen**.

5.4. Dashboard

Um das Dashboard aufzurufen, klicken Sie auf das Menüsymbol ☰ in der Seitenleiste und wählen Sie **Dashboard**.

Hier finden Sie eine Übersicht über Ihre Verbindungsdauer, das Volumen des gesicherten Datenverkehrs und die VPN-Server, mit denen Sie die meiste Zeit verbunden waren.

Hinweis
Diese Funktion ist derzeit nur auf Windows-Geräten verfügbar.


Bitdefender VPN
Dashboard
Last Session:
Connection time
0h 3m 21s
of protection and privacy
Secured traffic
2.87 MB
2.58 MB
296 KB
Top connected locations
Romania
0h 5m 35s
United States
0h 3m 21s

6. EINSTELLUNGEN & FUNKTIONEN VON BITDEFENDER VPN

6.1. Einstellungen aufrufen

Die Bitdefender VPN-Einstellungen finden Sie auf folgendem Wege:

- **Unter Windows**
  1. Öffnen Sie Bitdefender VPN, indem Sie auf das Symbol in der Taskleiste doppelklicken oder indem Sie mit der rechten Maustaste darauf klicken und „Anzeigen“ wählen.
  2. Klicken Sie links auf die Schaltfläche **Einstellungen** (ein Zahnradsymbol).

- **Unter macOS**
  1. Öffnen Sie Bitdefender VPN auf Ihrem macOS-Gerät, indem Sie in der Menüleiste auf das entsprechende Symbol klicken.
  2. Klicken Sie rechts oben in der Bitdefender VPN-Oberfläche auf das Zahnradsymbol und wählen Sie „Einstellungen“.

- **Unter Android**
  1. Öffnen Sie die Bitdefender VPN-App auf Ihrem Gerät.
  2. Klicken Sie rechts oben in der Bitdefender VPN-Oberfläche auf das Zahnradsymbol.

- **Unter iOS**
  1. Öffne das Bitdefender VPN App auf Ihrem Gerät.
  2. Klicken Sie auf die Zahnradschaltfläche in der oberen rechten Ecke des Bitdefender VPN Schnittstelle.

6.2. Funktionen

6.2.1. Autom. verbinden

Egal ob unterwegs, bei der Arbeit in einem Café oder beim Warten am Flughafen: Oftmals ist es am bequemsten, sich mit einem öffentlichen

WLAN zu verbinden, um Zahlungen anzuweisen, E-Mails abzurufen oder einen schnellen Blick in soziale Netzwerke zu werfen. Aber hier können auch Datenjäger lauern, die nur darauf warten, dass Ihre persönlichen Daten durch das Netzwerk wandern.

Zum Schutz vor den Gefahren ungesicherter oder unverschlüsselter öffentlicher WLAN-Hotspots verfügt Bitdefender VPN über die Funktion zur automatischen Verbindungsherstellung. Damit wird Bitdefender VPN, je nach Ihren vorgenommenen Einstellungen und Ihrem Betriebssytem, in bestimmten Situationen automatisch aktiviert.

- Unter **Windows** kann die Funktion zur automatischen Verbindungsherstellung für die folgenden Szenarien aktiviert werden:
  - **Start:** Mit VPN beim Start von Windows verbinden.
  - **Ungesichertes WLAN:** Das VPN bei allen Verbindungen mit öffentlichen oder ungesicherten WLAN-Netzwerken verwenden.
  - **Peer-to-Peer-Apps:** VPN-Verbindung herstellen, wenn eine Peer-to-Peer-Filesharing-App gestartet wird.
  - **Apps und Domänen:** Das VPN grundsätzlich für bestimmte Apps und Websites verwenden.

    Hinweis

    1. Klicken Sie auf den **Verwalten**-Link.
    2. Suchen Sie nach der App, für die Sie das VPN verwenden möchten, markieren Sie den Namen der App und klicken Sie dann auf **Hinzufügen**.

  - **Website-Kategorien:** VPN-Verbindung beim Besuch bestimmter Website-Kategorien herstellen. Bitdefender VPN kann automatische Verbindungen für die folgenden Website-Kategorien herstellen:
    - Finanzen
    - Online-Zahlungen
    - Gesundheitswesen
    - Filesharing
    - Online-Partnersuche

- Nicht jugendfreie Inhalte

> **Hinweis**
> Sie können für jede Kategorie einen anderen Server auswählen, mit dem sich das VPN verbinden soll.

- Unter **macOS** kann die Funktion zur automatischen Verbindungsherstellung für die folgenden Szenarien aktiviert werden:
  - **Start:** Mit VPN beim Start von macOS verbinden.
  - **Ungesichertes WLAN:** Verwenden Sie das VPN, wenn Sie sich mit öffentlichen oder ungesicherten WLAN-Netzwerken verbinden.
  - **Peer-to-Peer-Apps:** Stellen Sie eine Verbindung zum VPN her, wenn Sie eine Peer-to-Peer-Dateifreigabe-App starten.
  - **Anwendungen:** Für bestimmte Apps immer eine VPN-Verbindung herstellen.
- Unter **Android** und **iOS**> kann die Funktion zur automatischen Verbindungsherstellung von Bitdefender VPN nur für Verbindungen mit ungesicherten oder öffentlichen WLAN-Netzwerken aktiviert werden.

6.2.2. Internet Kill-Switch

Die Not-Aus-Funktion ist eine weitere Neuerung in Bitdefender VPN. Wenn diese Funktion aktiviert ist, wird sämtlicher Internet-Datenverkehr gestoppt, falls die VPN-Verbindung aus irgend einem Grund abreißen sollte. Sobald der Zugang zum Internet wieder steht, wird die VPN-Verbindung wieder hergestellt.

So aktivieren Sie die Not-Aus-Funktion:

- **Unter Windows**
  1. Öffnen Sie die Bitdefender VPN-App auf Ihrem Gerät, indem Sie auf das entsprechende Symbol in der Taskleiste doppelklicken oder mit der rechten Maustaste darauf klicken und **Anzeigen** auswählen.
  2. Klick auf das **Einstellungen** Schaltfläche (dargestellt durch ein Zahnrad) auf der linken Seite der Benutzeroberfläche.
  3. Wählen Sie **Erweitert**.

4. Aktivieren Sie die Option **Internet-Not-Aus**.

- **Auf Android**
  1. Öffne das Bitdefender VPN App auf Ihrem Gerät.
  2. Klicken Sie auf die Zahnradschaltfläche in der oberen rechten Ecke des Bitdefender VPN Schnittstelle.
  3. Aktivieren Sie unter **Einstellungen** die Option **Internet-Not-Aus**.

- **Auf iOS**
  1. Öffne das Bitdefender VPN App auf Ihrem Gerät.
  2. Klicken Sie auf die Zahnradschaltfläche in der oberen rechten Ecke des Bitdefender VPN Schnittstelle.
  3. Unter **Einstellungen**, aktivieren Sie die **Notausschalter** Möglichkeit.

> **Hinweis**
> Diese Funktion ist auch für macOS-Geräte ab Betriebssystemversion 10.15.4 verfügbar.

6.2.3. Split Tunneling

Das Split Tunneling in Ihrem VPN ist eine Funktion, mit der Sie einen Teil des Datenverkehrs Ihrer Geräte und Anwendungen durch ein verschlüsseltes VPN leiten können, während andere Anwendungen oder Geräte direkt auf das Internet zugreifen. Dies ist zum Beispiel nützlich, wenn Sie Dienste nutzen möchten, die für eine ordnungsgemäße Funktion Ihren Standort benötigen, gleichzeitig aber potenziell sensible Kommunikationsverbindungen und Daten absichern möchten.

Wenn Sie die Funktion **Split Tunneling** aktivieren, umgehen ausgewählte Apps und Websites das VPN und greifen direkt auf das Internet zu.

Gehen Sie wie folgt vor, um die Anwendungen und Websites zur Umgehung des VPNs festzulegen:

1. Klicken Sie nach Aktivierung der Funktion auf den **Verwalten**-Link.
2. Klicken Sie auf **Hinzufügen**.
3. Suchen Sie nach der jeweiligen Anwendung bzw. geben Sie die URL der gewünschten Website ein und klicken Sie auf **Hinzufügen**.

Hinweis
Wenn Sie eine Website hinzufügen, gilt die Umgehung für die gesamte Domäne einschließlich aller Unterdomänen.

Wichtig
Auf **macOS**-Geräten ist das Split Tunneling nur für Websites verfügbar.

6.2.4. App Traffic Optimizer

Mit dem App Traffic Optimizer in Bitdefender VPN können Sie den Datenverkehr für die wichtigsten Apps auf Ihrem Gerät priorisieren, ohne dass Sie mit Ihrer Verbindung Risiken für Ihre Privatsphäre eingehen. VPNs leiten den Internetverkehr durch einen sicheren Tunnel um und schützen ihn mit zuverlässigen Verschlüsselungsalgorithmen.

Die Kombination dieser Verfahren kann jedoch auch Nachteile haben, vor allem mit Blick auf die Verbindungsgeschwindigkeit. Dabei kann die Verbindung durch verschiedene Faktoren ausgebremst werden. Die häufigsten sind die Entfernung zum genutzten Server, Netzwerküberlastungen und eine hohe Bandbreitennutzung. Haben auch Sie eine VPN-Verbindung schon unterbrochen, weil Sie einfach zu langsam war? Damit ist mit Bitdefender VPN jetzt Schluss.

Wie funktioniert der App Traffic Optimizer?

Bestimmte Anwendungen und Dienste, so z. B. Streaming-Plattformen, Torrent-Clients und Spiele, benötigen mehr Bandbreite. Eine Dauernutzung könnte sich also negativ auf Ihre Verbindungsgeschwindigkeit auswirken. Mit der Nutzung eines VPN-Tunnels geht naturgemäß schon eine gewisse Verlangsamung Ihrer Verbindung einher; eine zusätzliche Belastung Ihrer Verbindung könnte Ihr Online-Erlebnis daher spürbar beeinträchtigen.

Der App Traffic Optimizer in Bitdefender VPN ist eine Funktion, die durch die Priorisierung von Apps Abhilfe bei langsamen VPN-Verbindungen schafft. Sie legen fest, welcher App die meiste Bandbreite erhalten soll, und die neue Funktion weist die Ressourcen entsprechend zu. Wenn Sie beispielsweise in einem Online-Meeting sind und feststellen, dass die Qualität Ihrer Verbindung nicht ausreicht, können Sie mit App Traffic Optimizer den Datenverkehr Ihrer Videokonferenz-Software priorisieren.

Normalerweise müssten VPN-Nutzer in diesem Fall alle störenden Prozesse auf ihrem Gerät schließen oder sogar ihre VPN-Verbindung

deaktivieren. Mit den App Traffic Optimizer müssen Sie nicht nie wieder zwischen Privatsphäre und Verbindungsgeschwindigkeit entscheiden.

App Traffic Optimizer richtig nutzen

Aktuell ist die Funktion nur auf Windows-Geräten verfügbar und ermöglicht es Ihnen, den Datenverkehr für bis zu drei Anwendungen zu priorisieren.

Und so können Sie die Funktion ganz einfach aktivieren und konfigurieren:

1. Starten Sie die Bitdefender VPN-Anwendung auf Ihrem Windows-Computer.
2. Klicken Sie auf die Schaltfläche in der Seitenleiste, um die VPN-Einstellungen aufzurufen.
3. Rufen Sie den Reiter **Allgemein** auf und aktivieren Sie die Funktion **App Traffic Optimizer**. Die Farbe des Schalters wechselt von grau zu blau.

So legen Sie die Anwendungen fest, die von dieser Funktion priorisiert werden:

1. Drücke den**Verwalten**Verknüpfung.
2. Suchen Sie nach der App, für die Sie den Datenverkehr optimieren möchten, markieren Sie den Namen der App und klicken Sie dann auf **Hinzufügen**. Die Anwendung wird danach im Abschnitt **Priorisiert** angezeigt.

   Hinweis
   Wenn Sie die Anwendung, die Sie priorisieren möchten, erst kürzlich geöffnet haben, können Sie alternativ auch auf die Schaltfläche "+" im Fenster App Traffic Optimizer klicken.

3. Trennen Sie die Verbindung zu Bitdefender VPN und stellen Sie sie wieder her, nachdem Sie Anwendungen hinzugefügt oder aus der Liste entfernt haben.

Um eine App aus dem App Traffic Optimizer zu entfernen, klicken Sie einfach auf das Symbol neben dem Namen der App.

6.2.5. Werbeblocker und Anti-Tracker

Diese Funktionen sollen Ihnen helfen, Ihre Privatsphäre zu wahren und das Internet in vollen Zügen zu genießen, ohne von aufdringlicher

Werbung und neugierigen Unternehmen belästigt zu werden. Sie helfen Ihnen dabei, Werbung zu blockieren und Online-Tracking zu unterbinden.

Werbeblocker

Der **Werbeblocker** blockiert Werbeanzeigen, Pop-ups, laute Videowerbung und Werbebanner. So können Websites schneller geladen, übersichtlicher angezeigt und sicherer genutzt werden.

So aktivieren Sie den Werbeblocker:

1. Suchen Sie in den **Einstellungen** die Funktion **Werbeblocker und Anti-Tracker**.
2. Klicken Sie auf den **Verwalten**-Link.
3. Setzen Sie den Schalter auf die Position **EIN**.

Anti-Tracker

Mit dem **Anti-Tracker** blockieren Sie Tracker, die von Werbetreibenden eingesetzt werden, um Ihre Online-Aktivitäten nachzuverfolgen und Profile von Ihnen zu erstellen. Einige Websites funktionieren möglicherweise nicht, wenn Tracker blockiert werden, aber durch Hinzufügen der URL zu Ihrer Whitelist können Sie hier Abhilfe schaffen.

So aktivieren Sie den Anti-Tracker:

1. Suchen Sie die **Werbeblocker und Antitracker** Funktion ein **Einstellungen**.
2. Klick auf das **Verwalten** Verknüpfung.
3. Schalten Sie den Schalter auf die um **AN** Position.

Whitelist

Einige Websites werden möglicherweise nicht ordnungsgemäß geladen, wenn Sie ihren Tracker-Code und ihre Werbung blockieren. Wenn Sie die URLs dieser Domänen zur Whitelist hinzufügen, kann dieses Problem zwar behoben werden, aber bedenken Sie, dass Ihnen beim Aufrufen dieser Websites Werbung angezeigt wird und Tracker-Code aktiv ist.

Gehen Sie wie folgt vor, um Websites hinzufügen, für die Sie die Anzeige von Werbung und die Verwendung von Trackern erlauben möchten:

1. Suchen Sie die **Werbeblocker und Antitracker** Funktion ein **Einstellungen**.
2. Klicken Sie auf den **Verwalten**-Link. Wechseln Sie dann zum Abschnitt Whitelist in diesem Fenster und klicken Sie auf den entsprechenden **Verwalten**-Link.
3. Klicken Sie auf **Website hinzufügen** und geben Sie die gewünschte URL ein.

7. BITDEFENDER VPN DEINSTALLIEREN

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

- **Bitdefender VPNvon Windows-Geräten deinstallieren**
  - Unter **Windows 7**:
    1. Klicken Sie auf **Start**, rufen Sie die **Systemsteuerung** auf und doppelklicken Sie auf **Programme und Funktionen**.
    2. Suchen Sie nach **Bitdefender VPN** und wählen Sie **Deinstallieren**.
       Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist.
  - Unter **Windows 8** und **Windows 8.1**:
    1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
    2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
    3. Finden **Bitdefender VPN** und auswählen **Deinstallieren**.
       Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist.
  - Unter **Windows 10** und **Windows 11**:
    1. Klicken Sie auf **Start** und danach auf **Einstellungen**.
    2. Klicken Sie in den Einstellungen auf das **System**-Symbol und wählen Sie **Installierte Anwendungen**.
    3. Finden **Bitdefender VPN** und auswählen **Deinstallieren**.
    4. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.
       Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist.

- **Von macOS-Geräten deinstallieren**
  1. Klicken Sie in der Menüleiste auf **Los** und wählen Sie **Anwendungen**.

2. Doppelklicken Sie auf den **Bitdefender**-Ordner.
3. Führen Sie **BitdefenderUninstaller** aus.
4. Markieren Sie im neuen Fenster das Kästchen neben **Bitdefender VPN** und klicken Sie dann auf **Deinstallieren**.
5. Geben Sie den Namen und das Passwort eines gültigen Administratorkontos ein und klicken Sie auf **OK**.
6. Zum Abschluss erhalten Sie eine Meldung, dass Bitdefender VPN erfolgreich deinstalliert wurde. Klicken Sie auf **Schließen**.

- **Von Android-Geräten deinstallieren**
  1. Öffnen Sie den **Play Store**.
  2. Suchen Sie nach **Bitdefender VPN**.
  3. Wählen Sie auf der Bitdefender VPN-Seite im App Store die Option **Deinstallieren**.
  4. Bestätigen Sie durch Antippen von **OK**.
- **Von iOS-Geräten deinstallieren**
  1. Halten Sie die Bitdefender VPN-App mit Ihrem Finger gedrückt.
  2. Wählen Sie **App löschen**.
  3. Tippen Sie auf **Löschen**.

8. HÄUFIG GESTELLTE FRAGEN

Wann sollte ich Bitdefender VPN verwenden?

Bei Aufrufen, Herunterladen oder Hochladen von Inhalten im Internet sollten Sie stets Vorsicht walten lassen. Um beim Surfen im Netz jederzeit geschützt zu sein, empfehlen wir die Nutzung des VPNs, 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, E-Mail-Adressen, Kreditkartendaten etc.)
- Ihre IP-Adresse verbergen möchten

Kann ich mit Bitdefender VPN eine Stadt auswählen?

Ja. Aktuell können Sie mit Bitdefender VPN für Windows, macOS, Android und iOS Städte auswählen. Diese Städte stehen Ihnen derzeit zur Auswahl:

- **USA:** Atlanta, Charlotte, Chicago, Dallas, Denver, Houston, Los Angeles, Miami, New York, Newark, Phoenix, Portland, San Jose, Seattle, Washington
- **Kanada:** Montreal, Toronto, Vancouver
- **UK:** London, Manchester

Kann Bitdefender VPN als eigenständige App installiert werden?

Die VPN-App wird automatisch zusammen mit Ihrer Bitdefender-Sicherheitslösung installiert, kann aber auch als eigenständige App über die Produktseite, den Google Play Store und den App Store installiert werden.

Gibt Bitdefender meine IP-Adresse und übertragenen persönlichen Daten an Dritte weiter?

Nein, mit Bitdefender VPN wird Ihre Privatsphäre zu 100 % gewahrt. So kann niemand (Werbeanbieter, Internetdienstleister, Versicherungen usw.) auf Ihre Online-Protokolle zugreifen.

Welcher Verschlüsselungsalgorithmus kommt zum Einsatz?

Bitdefender VPN verwendet auf allen Plattformen das Hydra-Protokoll, eine 256-Bit-AES-Verschlüsselung bzw. die höchste sowohl vom Client als auch vom Server unterstützte Verschlüsselung mit Perfect Forward Secrecy. Das bedeutet, dass die Verschlüsselungsschlüssel für jede neue VPN-Sitzung erzeugt und nach Beendigung der Sitzung aus dem Speicher gelöscht werden.

Kann ich auf Inhalte mit regionalen Zugangsbeschränkungen zugreifen?

Mit Premium VPN erhalten Sie Zugriff auf ein ausgedehntes Netzwerk mit virtuellen Standorten in aller Welt.

Wird es die Akkulaufzeit meines Geräts beeinträchtigen?

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 verlangsamt das VPN meine Internetverbindung?

Bitdefender VPN ist auf einen ressourcenschonenden Betrieb beim Surfen im Netz ausgelegt. Abhängig von der Entfernung zwischen Ihrem tatsächlichen Standort und dem Standort des Servers, mit dem Sie eine Verbindung aufbauen, sind geringfügige Geschwindigkeitseinbußen jedoch zu erwarten. Sie fallen in der Regel aber so gering aus, dass sie bei normaler Online-Nutzung unbemerkt bleiben. 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 Pakistan), sollten Sie in solchen Fällen dem 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.