Bitdefender®

PASSWORD MANAGER

BENUTZERHANDBUCH

Bitdefender Password Manager

Bedienungsanleitung

Veröffentlichungsdatum: 21.11.2022

Impressum

Bitdefender

Inhaltsverzeichnis

ÜBER DIESE ANLEITUNG

Zielsetzung und Zielgruppe

Dieses Bitdefender Password ManagerHandbuch behandelt alle unterstützten Betriebssysteme (Windows, macOS, Android, iOS) und richtet sich an alle Bitdefender-Benutzer, die sich für den Einsatz von zur Verwaltung ihre Passwörter entschieden haben. Die enthaltenen Informationen setzen keine besonderen Computerkenntnisse voraus, sondern dienen allen Benutzern als leicht verständliche und hilfreiche Anleitung.

Wir stellen Ihnen alle Funktionen und Merkmale im Detail vor, um Ihnen eine optimale Nutzung unseres ultrasicheren und funktionsreichen Passwortmanagers zu ermöglichen.

Viel Spaß mit diesen nützlichen und informativen Handbuch.

Über dieses Handbuch

Dieses Handbuch behandelt die folgenden Themengebiete:

Erste Schritte (Seite 5)

Installation und erste Schritte mit Bitdefender Password Manager.

Funktionen und Merkmale (Seite 18)

Lernen Sie, wie man Bitdefender Password Manager und alle seine Funktionen optimal einsetzt.

Hilfe und Support (Seite 30)

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 PASSWORD MANAGER

Bitdefender Password Manager ist ein plattformübergreifender Dienst, mit dem Benutzer ihre Online-Passwörter speichern und verwalten können. Auf Grundlage der besten und sichersten bekannten Verschlüsselungsalgorithmen gewährleistet er ein Höchstmaß an Sicherheit. Er ist sowohl als mobile App als auch als Browsererweiterung verfügbar und dient Benutzern als geräteübergreifende Lösung für die Verwaltung von Identität, Passwörtern, Online-Banking und allen anderen Arten sensibler Daten.

Bitdefender Password Manager kann Ihre Passwörter für alle Websites und Online-Dienste mithilfe eines einzigen Master-Passworts automatisch speichern, automatisch ausfüllen, generieren und verwalten. So wird die Verwaltung Ihrer digitalen Identität zum Kinderspiel.

1.1. So wird die Sicherheit gewährleistet

Die Bitdefender Password Manager-Software stützt sich auf modernste Verschlüsselungsalgorithmen, die bestmögliche Datensicherheit gewährleisten, so z. B. AES-256-CCM, SH512 und BCRYPT sowie HTTPS- und WSS-Protokolle für die Datenübertragung. Alle beteiligten Daten werden jederzeit lokal ver- und entschlüsselt. So hat ausschließlich der Kontoinhaber Zugang zu den unter dem Benutzerkonto gespeicherten Informationen sowie zum Master-Passwort, das für den Zugang und die anschließende Nutzung der betreffenden Daten verwendet wird.

1.2. Password Manager: Testversion und kostenpflichtige Version

Der Funktionsumfang der Testversion von Bitdefender Password Manager ist identisch mit der kostenpflichtigen Version des Produkts, kann nach Aktivierung aber nur 90 Tage lang genutzt werden.

> **Notiz**
> Beachten Sie, dass die kostenpflichtige Version des Produkts zwar als eigenständiges Produkt erworben werden kann, der unbegrenzte Zugriff auf den Password Manager jedoch auch in den Abonnements von Bitdefender Premium Security und Bitdefender Ultimate Security enthalten ist.

2. ERSTE SCHRITTE

2.1. Systemanforderungen

Sie können die neueste Version von Bitdefender Password Manager nur auf Geräten mit den folgenden Betriebssystemen nutzen:

- **Für PC-Benutzer:**
  - Windows 7 mit Service Pack 1
  - Windows 8
  - Windows 8.1
  - Windows 10
  - Windows 11
- **Für macOS-Benutzer:**
  - macOS 10.14 (Mojave) und neuere macOS-Betriebssysteme

  Notiz
  Bitte beachten Sie, dass die Systemleistung auf Geräten mit Prozessoren älterer Generationen beeinträchtigt sein kann.
- **Für iOS-Benutzer:**
  - iOS 11.0 oder neuere iOS-Betriebssysteme
- **Für Android-Benutzer:**
  - Android 5.1 und neuere Android-Betriebssysteme

  Notiz
  - Die Funktion zum Entsperren per Fingerabdruck wird ab **Android 6.0** unterstützt.
  - Die Funktion für das automatische Einfügen wird ab **Android 8.0** unterstützt und ist mit iPhone, iPad und iPod touch kompatibel.

2.1.1. Software-Anforderungen

Um Bitdefender Password Manager und alle Funktionen nutzen zu können, müssen Ihre Windows- oder macOS-Geräte die folgenden Softwareanforderungen erfüllen:

- **Microsoft Edge** (basierend auf Chromium 80 und höher)
- **Mozilla Firefox** (ab Version 65)
- **Google Chrome** (ab Version 72)
- **Safari** (ab Version 12)

> **Notiz**
> Die Softwareanforderungen gelten nicht für Android und iOS.

> **Warnung**
> Werden diese Systemanforderungen nicht erfüllt, ist die Bitdefender Password Manager-Installation nicht möglich oder es kommt zu Fehlfunktionen des Produkts.

2.2. Installation

In diesem Kapitel erfahren Sie, wie Sie den {1}{2} in den Webbrowsern unter Windows und macOS sowie auf Ihren Android- oder iOS-Geräten installieren.

> **Wichtig**
> Stellen Sie vor der Installation sicher, dass Sie über ein gültiges Password Manager-Abonnement in Ihrem **Bitdefender Central**-Konto verfügen, damit diese Browsererweiterung die Gültigkeit über Ihr Konto bestätigen kann.
>
> Sie finden Ihre aktiven Abonnements in Bitdefender Central unter **Meine Abonnements**.

2.2.1. Installation auf Windows- und macOS-Geräten

Anders als die meisten Desktop-Anwendungen und Softwarelösungen, die auf diesen Geräten installiert und eingerichtet werden müssen, wird der Bitdefender Password Manager als Browsererweiterung - auch Add-on genannt - bereitgestellt, die im Handumdrehen zu Ihrem bevorzugten Browser hinzugefügt und aktiviert werden kann.

Das Produkt unterstützt derzeit die folgenden Browser: **Google Chrome**, **Mozilla Firefox**, **Microsoft Edge** und **Safari**.

1. Rufen Sie https://central.bitdefender.com/ auf und melden Sie sich bei Ihrem Benutzerkonto an.
   Wenn Sie noch kein Konto haben, klicken Sie auf **Benutzerkonto erstellen** und geben Sie dann Ihren vollständigen Namen, eine E-Mail-Adresse und ein Passwort ein.
2. Klicken Sie im Menü links auf **Meine Geräte**.
3. Klicken Sie unter **Meine Geräte** auf **+ Gerät hinzufügen**.
4. Dadurch wird ein neues Fenster geöffnet. Klicken Sie hier auf **Password Manager**.
5. Klicken Sie auf **Dieses Gerät**.
   Wenn Sie die Installation auf einem anderen Gerät vornehmen möchten, klicken Sie auf Weitere Geräte. Sie können dann einen Download-Link per E-Mail an das jeweilige Gerät senden oder die URL für die Installation selbst kopieren.
6. Wählen Sie anschließend den Browser aus, für den Sie die Password Manager-Erweiterung installieren möchten.
7. Über die entsprechende Schaltfläche gelangen Sie direkt zum Erweiterungsangebot des Browsers. Folgen Sie dort einfach den Anweisungen auf dem Bildschirm, wie im Folgenden gezeigt:

   Microsoft Edge

   - Klicken Sie auf **Abrufen**.
   - Klicken Sie jetzt auf **Erweiterung hinzufügen**.

   Google Chrome

   - Klicken Sie auf **Chrome hinzufügen**.
   - Klicken Sie im Bestätigungsfeld auf **Erweiterung hinzufügen**.

   Mozilla Firefox

   - Klicken Sie auf **Zu Firefox hinzufügen**.
   - Klicken Sie oben rechts im Fenster auf **Installieren**.

   Safari

   - Klicken Sie auf **Laden** und danach auf **Installieren**.

- Öffnen Sie Safari und klicken Sie im Menü oben auf **Einstellungen**.
- Klicken Sie in den Einstellungen auf den Reiter **Erweiterungen**.
- Markieren Sie das Kontrollkästchen neben dem Password Manager, um ihn zu aktivieren.

Legen Sie nach Abschluss dieser Schritte ein sicheres Master-Passwort fest und klicken Sie auf **Master-Passwort speichern**, nachdem Sie die **Nutzungsbedingungen** gelesen und akzeptiert haben.

Wichtig
Bitte beachten Sie, dass Sie dieses Master-Passwort benötigen, um auf die im Bitdefender Password Manager gespeicherten Passwörter, Kreditkarteninformationen und Notizen zuzugreifen. Das Master-Passwort dient als Schlüssel, der eine Nutzung des Produkts erst möglich macht.

Warnung
Nach Erstellung des Master-Passworts erhalten Sie einen **24-stelligen Wiederherstellungsschlüssel**. **Bewahren Sie Ihren Wiederherstellungsschlüssel an einem sicheren Ort auf und verlieren Sie ihn nicht**. Dieser Schlüssel ist die einzige Möglichkeit, auf Ihre im Password Manager gespeicherten Passwörter zuzugreifen, sollten Sie das zuvor für Ihr Konto eingerichtete **Master-Passwort vergessen**.

- Klicken Sie danach auf **Schließen**.

2.2.2. Installation auf Android-Geräten

Der Bitdefender Password Manager lässt sich auf Android-Telefonen und -Tablets am einfachsten installieren, indem Sie die App direkt von Google Play herunterladen.

GET IT ON Google Play

Sie können die Bitdefender Password Manager-App aber auch über Ihr **Bitdefender Central**-Konto installieren:

1. Melden Sie sich dazu auf Ihrem Android-Mobilgerät bei Ihrem Bitdefender Central-Konto an, indem Sie https://login.bitdefender.com/central/login aufrufen.
2. Wählen **Meine Geräte** in der linken Seitenleiste des Bildschirms.

3. Im **Meine Geräte** Abschnitt, fahren Sie fort, indem Sie auf klicken **+ Gerät hinzufügen**.
4. Diese Aktion wird dazu führen, dass ein neues Fenster erscheint. Wählen **Passwortmanager** im Selektionsbild.
5. Wählen **Dieses Gerät**.
   Wenn Sie die Installation auf einem anderen Gerät vornehmen möchten, klicken Sie auf **Weitere Geräte**. Sie können dann einen Download-Link per E-Mail an das jeweilige Gerät senden oder die URL für die Installation selbst kopieren.
6. Sie werden zu **Google Play** weitergeleitet. Tippen Sie auf **Installieren**, um dem Bitdefender Password Manager auf Ihr Android herunterzuladen.
7. Öffnen Sie nach Abschluss des Downloads die Password Manager-App.
8. Wenn Sie nicht automatisch bei Ihrem Konto angemeldet werden, melden Sie sich mit Ihrem Benutzernamen und Passwort an.
   Nachdem Sie diese Schritte befolgt haben, legen Sie ein starkes Master-Passwort fest und drücken Sie dann die **Master-Passwort speichern** Schaltfläche, nachdem Sie gelesen haben und damit einverstanden sind **Geschäftsbedingungen**.

   Wichtig
   Beachten Sie, dass Sie dieses Master-Passwort benötigen, um alle im Bitdefender Password Manager gespeicherten Passwörter, Kreditkarteninformationen und Notizen freizuschalten. Dies ist im Wesentlichen der Schlüssel, der es dem Besitzer ermöglicht, dieses Produkt zu verwenden.

   Warnung
   Beim Erstellen des Master-Passworts erhalten Sie eine **24-stelliger Wiederherstellungsschlüssel**. Notieren Sie sich Ihren Wiederherstellungsschlüssel an einem sicheren Ort und verlieren Sie ihn nicht. Dieser Schlüssel ist die einzige Möglichkeit, auf Ihre in Password Manager gespeicherten Passwörter zuzugreifen, falls dies doch passieren sollte **vergessen Sie das Master-Passwort** zuvor für Ihr Konto eingerichtet.

   - Sie können drücken **Schließen** wenn fertig.

9. Legen Sie eine **4-stellige PIN** fest. Wenn Sie jetzt zu einer anderen App wechseln und dann zum Password Manager zurückkehren, müssen Sie so das zuvor eingerichtete Master-Passwort nicht erneut eingeben. Falls verfügbar, können Sie auch die Gesichtserkennung oder die Authentifizierung per Fingerabdruck aktivieren.
10. Tippen Sie auf **Automatisches Ausfüllen aktivieren**, um die Android-Einstellungen für das automatische Ausfüllen zu konfigurieren.

    > **Notiz**
    > Wenn Sie diesen Schritt überspringen, können Sie die Android-Funktion zum automatischen Ausfüllen auch zu einem späteren Zeitpunkt aktivieren und anpassen, indem Sie die Anweisungen unter Intelligentes automatisches Ausfüllen (Seite 19) befolgen.

11. Es wird eine Liste mit Anwendungen angezeigt, die Passwörter automatisch ausfüllen können.
    Wählen Sie **Password Manager** und bestätigen Sie dann, dass Sie dieser App vertrauen.
    Tippen Sie auf **OK**.
12. Geben Sie die PIN ein, die Sie in **Schritt 9** eingerichtet haben, um diese Aktion zu bestätigen.

Die Installation auf Ihrem Android-Gerät ist damit abgeschlossen.

2.2.3. Installation auf iOS-Geräten

Der Bitdefender Password Manager lässt sich auf iOS- und iPadOS-Geräten am einfachsten installieren, indem Sie die App direkt aus dem App Store herunterladen.

Download on the App Store

Die Installation der Bitdefender Password Manager-App kann auch über Ihren erfolgen Bitdefender-Zentrale Konto:

1. Melden Sie sich dazu auf Ihrem iPhone oder iPad bei Ihrem Bitdefender Central-Konto an, indem Sie https://login.bitdefender.com/central/login aufrufen.
2. Wählen **Meine Geräte** in der linken Seitenleiste des Bildschirms.

3. Im **Meine Geräte** Abschnitt, fahren Sie fort, indem Sie auf klicken **+ Gerät hinzufügen**.
4. Diese Aktion wird dazu führen, dass ein neues Fenster erscheint. Wählen **Passwortmanager** im Selektionsbild.
5. Wählen **Dieses Gerät**.
   Wenn Sie auf einem anderen Gerät installieren möchten, wählen Sie **Andere Geräte**. Sie können dann einen Download-Link per E-Mail an das jeweilige Gerät senden oder die URL für die Installation direkt kopieren.
6. Sie werden zum **App Store** weitergeleitet. Tippen Sie auf das Wolkensymbol mit einem nach unten zeigenden Pfeil, um den Bitdefender Password Manager für iOS herunterzuladen.
7. Öffnen Sie nach Abschluss der Installation die Bitdefender App und markieren Sie das kleine Kästchen auf dem Bildschirm. Wählen Sie **Fortfahren**, nachdem Sie die **Nutzungsbedingungen** gelesen und akzeptiert haben.
8. Wenn Sie nicht automatisch bei Ihrem Konto angemeldet werden, melden Sie sich mit Ihrem Benutzernamen und Passwort an.
   Nachdem Sie diese Schritte befolgt haben, legen Sie ein starkes Master-Passwort fest und drücken Sie dann die **Master-Passwort speichern** Schaltfläche, nachdem Sie gelesen haben und damit einverstanden sind **Geschäftsbedingungen**.

> **Wichtig**
> Beachten Sie, dass Sie dieses Master-Passwort benötigen, um alle im Bitdefender Password Manager gespeicherten Passwörter, Kreditkarteninformationen und Notizen freizuschalten. Dies ist im Wesentlichen der Schlüssel, der es dem Besitzer ermöglicht, dieses Produkt zu verwenden.

Warnung

Beim Erstellen des Master-Passworts erhalten Sie eine **24-stelliger Wiederherstellungsschlüssel**. Notieren Sie sich Ihren Wiederherstellungsschlüssel an einem sicheren Ort und verlieren Sie ihn nicht. Dieser Schlüssel ist die einzige Möglichkeit, auf Ihre in Password Manager gespeicherten Passwörter zuzugreifen, falls dies doch passieren sollte **vergessen Sie das Master-Passwort** zuvor für Ihr Konto eingerichtet.

- Sie können drücken **Schließen** wenn fertig.

9. Ein ... kreieren **4-stellige PIN**, wenn Sie also zu einer anderen App wechseln und dann zu Password Manager zurückkehren, müssen Sie das zuvor eingerichtete Master-Passwort nicht erneut eingeben. Falls verfügbar, können Sie auch die Gesichtserkennung oder die Authentifizierung per Fingerabdruck aktivieren.

Die Installation auf Ihrem iOS/iPadOS-Gerät ist damit abgeschlossen.

3. IMPORT UND EXPORT IHRER PASSWÖRTER

Mit dem Bitdefender Password Manager ist die Kommunikation und der Austausch von Daten mit externen Quellen, Plattformen und Software-Tools problemlos möglich. So ist gewährleistet, dass die häufige Anforderung hinsichtlich des Imports bzw. Exports von Passwörtern in bzw. aus dem Bitdefender Password Manager mühelos erfüllt wird.

3.1. Produktkompatibilität

Der Bitdefender Password Manager ermöglicht eine nahtlose Datenübertragung aus den folgenden Anwendungen:

- **1Password**
- **Bitwarden**
- **Bitdefender Password Manager**
- **ByePass**
- **Chrome browser**
- **Claro**
- **Dashlane**
- **Edge browser**
- **ESET Password Manager v2**
- **ESET Password Manager v3**
- **StickyPassword**
- **Watchguard**
- **Firefox browser**
- **Gestor de contraseñas – Claro**
- **Gestor de contraseñas – SIT**
- **Gestor de contraseñas – Telnor**
- **KeePass 2.x**
- **LastPass**
- **Panda Dome Passwords**

- **PassWatch**
- **Saferpass**
- **SFR Cybersécurité**
- **SIT**
- **F-Secure**
- **Telnor**

> **Notiz**
> Wenn der Name des Browsers oder des Passwortmanagers, aus dem Sie Daten übertragen möchten, nicht in der Liste aufgeführt ist, erfahren Sie in unserer Online-Anleitung, wie Sie eine CSV-Datei mit Daten aus nicht unterstützten Passwortmanagern erstellen und bearbeiten können, um sie dann in den **Bitdefender Password Manager** zu importieren: https://www.bitdefender.de/consumer/support/answer/12244/

Dieser Datentransfer zwischen dem Bitdefender Password Manager und anderen Lösungen kann über die folgenden Datenformate erfolgen:

CSV, **JSON**, **XML**, **TXT**, **1pif** und **FSK**.

3.2. Import in den Password Manager

Der Bitdefender Password Manager ermöglicht Ihnen den einfachen Import von Passwörtern aus anderen Passwortmanagern und Browsern. Wenn Sie von einem anderen Passwortverwaltungsdienst zu Bitdefender Password Manager wechseln möchten, haben Sie dort vermutlich eine beträchtliche Menge an Anmeldedaten wie Benutzernamen, Passwörter und andere Login-Informationen für Ihre Konten gespeichert.

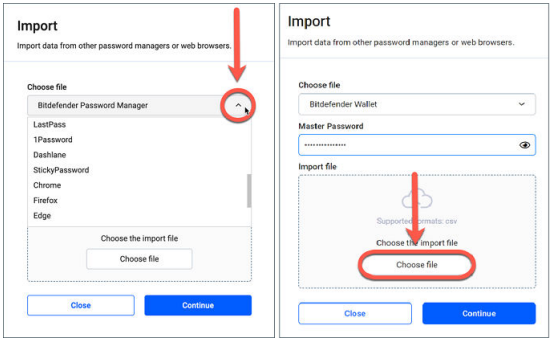
Mit dem Umstieg auf den Bitdefender Password Manager möchten Sie diese gespeicherten Daten bestimmt auch mitnehmen.

Gehen Sie zum Import Ihrer gespeicherten Daten aus anderen Anwendungen und Webbrowsern in den Bitdefender Password Manager wie folgt vor, **unabhängig vom Betriebssystem**, auf dem Sie dieses Produkt installiert haben:

1. Klicken Sie auf das Password Manager-Symbol in Ihrem Webbrowser (unter Windows und macOS) oder starten Sie die Password Manager-

App (unter Android und iOS). Geben Sie nach Aufforderung Ihr **Master-Passwort** ein.

2. Öffnen Sie das Passwort Manager-Menü , um die Menüleiste links einzublenden und klicken Sie auf den Menüpunkt **Einstellungen**.
3. Scrollen Sie nach unten zum Abschnitt **Daten** und klicken Sie auf die Option **Daten importieren**.
4. Wählen Sie im Dropdown-Menü den Namen der Passwortmanager-Anwendung oder des Browsers, aus dem Sie Ihre Konten importieren möchten. Geben Sie Ihr **Master-Passwort** in das entsprechende Feld ein und klicken Sie dann auf **Datei wählen**.



5. Durchsuchen Sie Ihre Ordner, um den Speicherort zu finden, an dem Sie die Datei mit Ihren Benutzernamen und Passwörtern gespeichert haben, die Sie aus Ihrem anderen Passwortmanager oder Webbrowser exportiert haben, und klicken Sie dann auf **Fortfahren**.

Nach dem Import sind Ihre Passwörter dann auf allen Geräten verfügbar, auf denen die Bitdefender Password Manager-App bzw. die Browsererweiterung installiert ist.

3.3. Export aus dem Password Manager

Mit dem Bitdefender Password Manager können Sie Ihre gespeicherten Passwörter (einschließlich Anmeldedaten, sichere Notizen usw.) ganz einfach in eine CSV-Datei (Comma-separated values) oder verschlüsselte

Datei exportieren. So möchten wir Ihnen den Umstieg so einfach wie möglich machen, sollten Sie vom vom Bitdefender Password Manager zu einem anderen Passwortmanager-Dienst wechseln möchten.

> **Wichtig**
> Eine CSV-Datei ist **nicht** verschlüsselt und enthält Benutzernamen und Passwörter im Klartextformat. Das bedeutet, dass Ihre privaten Informationen von jedem gelesen werden können, der Zugriff auf Ihr Gerät hat. Wir empfehlen Ihnen daher, die folgenden Schritte nur auf einem vertrauenswürdigen Gerät durchzuführen.

So exportieren Sie Ihre Daten aus dem Bitdefender Password Manager:

1. Klicken Sie in Ihrem Webbrowser (unter Windows oder macOS) auf das Password Manager-Symbol oder starten Sie die Password Manager-Anwendung (unter Android oder iOS). Wenn Sie dazu aufgefordert werden, geben Sie Ihre ein Master Passwort.
2. Öffnen Sie das Passwort Manager-Menü, um die Menüleiste links einzublenden und klicken Sie auf den Menüpunkt **Einstellungen**.
3. Scrollen Sie nach unten zum Abschnitt **Daten** und klicken Sie auf die Option **Daten exportieren**.
4. Ihnen sollten nun die folgenden beiden Optionen angezeigt werden:
   - **CSV**
   - **Passwortgeschützte Dateien**

   Wählen Sie die gewünschte Option, geben Sie Ihr Master-Passwort ein und klicken Sie auf **Daten exportieren**.

   > **Notiz**
   > Wenn Sie die Option "Passwortgeschützte Datei" wählen, werden Sie aufgefordert, die Daten mit der Liste Ihrer Konten mit einem Passwort zu verschlüsseln, so dass nur Sie bei Bedarf darauf zugreifen können.

5. Ihr Webbrowser/Ihre App speichert eine Datei mit dem Namen `Bitdefender Password Manager_exported_data_aktuelles-datum` auf Ihrem System im Standard-Download-Ordner. Sie enthält alle Ihre im Bitdefender Password Manager gespeicherten Daten.

Nach dem Export Ihrer Daten können Sie diese in einen Passwortmanager Ihrer Wahl hochladen.

4. FUNKTIONEN UND MERKMALE

In diesem Kapitel lernen Sie alle Merkmale und Funktionen des Bitdefender Password Managers kennen und erfahren wofür und wie man Sie optimal einsetzt.

4.1. Richtiger Umgang mit Passwörtern

4.1.1. Passwortgenerator

Die wichtigste Regel für mehr Sicherheit im Internet ist die konsequente Nutzung von zufällig gewählten Passphrasen für jeden Dienst, für den ein Benutzerkonto erstellt werden muss. Dabei darf jede Passphrase immer nur einmal vergeben werden. Die Wiederverwendung von Passwörtern über mehrere Dienste hinweg ist die Hauptursache für Identitätsdiebstahl und andere Schäden im Zusammenhang mit der betrügerischen Übernahme von Konten.

Diese Funktion hilft Benutzern bei der Erstellung sicherer, komplexer und einzigartiger Passwörter für jedes neue Online-Benutzerkonto. Sie müssen nie sich nie wieder selbst sichere Passwörter ausdenken und merken oder darauf achten, das gleiche Passwort nicht mehrfach zu vergeben.

Sie finden den **Passwortgenerator** im entsprechenden Reiter oben in der Password Manager-Benutzeroberfläche.

Der Generator gibt je nach Einstellung Passwörter **mit 4 bis 32 Zeichen** aus.

Sie können auch festlegen, welche Arten von Zeichen im zufällig generierten Passwort enthalten sein sollen oder nicht, indem Sie die entsprechenden Kästchen aktivieren oder deaktivieren. **(Kleinbuchstaben, Großbuchstaben, Zahlen, Sonderzeichen)**

Klicken Sie auf die Schaltfläche rechts neben dem angezeigten Passwort, um das vorgeschlagene Passwort zu ändern.

Wenn Sie das angezeigte Passwort verwenden möchten, klicken Sie auf **Passwort verwenden**. Die Zeichenfolge wird in der Zwischenablage gespeichert.

Notiz
Ihre zuvor erstellten Passwörter werden vorübergehend im Passwortverlauf gespeichert, auf den Sie über die Schaltfläche **Passwortverlauf** zugreifen können.

4.1.2. Passworterfassung

Mit dieser Funktion im Password Manager werden Sie aufgefordert, alle neuen Passwörter sofort nach der Erstellung zu speichern. Der Password Manager fordert Benutzer auf, ihre neu erstellten Passwörter zu speichern, damit sie sofort der von Bitdefender bereitgestellten ultrasicheren Umgebung hinzugefügt werden können.

4.1.3. Intelligentes automatisches Ausfüllen

Der Bitdefender Password Manager kann so eingerichtet werden, dass er Ihre Anmeldedaten und vor allem Ihre Passwörter automatisch ausfüllt. Von uns entwickelte Algorithmen erkennen bereits besuchte Websites und füllen Ihre Anmeldedaten für Sie aus, so dass Sie bei jeder Anmeldung bei Ihren Diensten Zeit sparen.

1. Klicken Sie unter Windows oder macOS auf das **Password Manager**-Symbol in Ihrem Webbrowser.
   Starten Sie unter Android oder iOS die **Password Manager**-App.
   Geben Sie nach Aufforderung Ihr **Master-Passwort** ein.
2. Öffnen Sie das Passwort Manager-Menü, um die Menüleiste links einzublenden und klicken Sie auf den Menüpunkt **Einstellungen**.
3. Klicken Sie auf **Geräteeinstellungen**.
4. Hier finden Sie eine Schaltfläche, die entweder **Automatisches Ausfüllen deaktivieren** oder **Automatisches Ausfüllen aktivieren** anzeigt. Diese Einstellung steuert den Betriebszustand der Funktion für das intelligente automatische Ausfüllen.

4.1.4. Sicherheitsbericht

Der Sicherheitsbericht ist ein Tool, das Berichte auf Grundlage verschiedener Funktionen erstellt, die Ihrer digitalen Sicherheit dienen. So werden Sie nach Bewertung der Sicherheit vorhandener Passwörter zum Beispiel informiert, ob ein Passwort Ihre sofortige Aufmerksamkeit erfordert. Auch doppelte Passwörter werden erkannt. Sie werden dann

aufgefordert, diese Passwörter entsprechend zu ändern, um die mit der Mehrfachnutzung verbundenen Risiken zu vermeiden.

Der Bericht liefert Ihnen hauptsächlich Informationen zu Ihren Passwortgewohnheiten, d. h. zu mehrfach genutzten Passwörtern, schwachen oder anderweitig kompromittierten Passwärtern und E-Mail-Adressen.

Dazu wird die Liste der verschlüsselten Hashes von Troys Website lokal auf Ihrem Gerät verglichen, um zu prüfen, ob sie die entsprechenden Hashes Ihrer Passwörter enthält. Wenn eine Übereinstimmung gefunden wird, werden Sie benachrichtigt, damit Sie Ihre Passwörter und andere Anmeldedaten ändern können.

Sie können den **Sicherheitsbericht** aufrufen, indem Sie den Password Manager öffnen und in der Menüleiste oben auf die entsprechende Schaltfläche klicken.

4.1.5. Plattformübergreifende Synchronisierung

Wenn Sie Ihre Passwörter einmal im Bitdefender Password Manager gespeichert haben, können Sie diese auch auf all Ihren Windows-, Mac-, Android- oder iOS-Geräten in Chrome, Safari, Firefox und Edge oder in den mobilen Apps speichern und jederzeit sicher darauf zugreifen.

> **Notiz**
> Bitdefender verfügt zudem über einen **Offlinemodus**. So können Sie jederzeit und von überall auf Ihre Passwörter zugreifen, auch wenn Sie einmal keinen Zugang zum Internet haben.

4.1.6. Löschen von Einträgen

Um gespeicherte Passwörter zu löschen, klicken Sie zuerst auf das Bearbeitungssymbol neben dem Eintrag, den Sie entfernen möchten. Die Einträge finden Sie im Reiter **Konten**. Scrollen Sie nach unten und klicken Sie auf **Löschen**. Sie werden gefragt, ob Sie das Konto wirklich entfernen möchten. Klicken Sie zur Bestätigung auf **Entfernen**.

4.2. Richtiger Umgang mit Konten

4.2.1. Authentifizierung

Die Authentifizierung im Bitdefender Password Manager erfolgt über die **PIN**, die bei der Installation des Produkts festgelegt wurde. (Bitte beachten Sie, dass die Funktion **Automatisch sperren** den Password Manager sperrt oder Sie nach einer gewissen Zeit der Inaktivität im Browser oder dem Schließen der mobilen App abmeldet).

Alternativ ist die Authentifizierung, falls verfügbar, auch durch biometrische Verfahren möglich, so z. B. durch **Fingerabdruck** oder **Gesichtserkennung**.

So **aktivieren oder deaktivieren** Sie die biometrische Authentifizierung:

1. Klicken Sie unter Windows oder macOS auf die **Password Manager** Symbol in Ihrem Webbrowser.
   Starten Sie unter Android oder iOS die **Password Manager** Anwendung.
   Wenn Sie dazu aufgefordert werden, geben Sie Ihre ein Master Passwort.
2. Öffnen Sie das Password Manager-Menü , um die Seitenleiste auf der linken Seite zu erweitern, und klicken Sie auf **Einstellungen** Menüpunkt.
3. Klicke auf **Geräteeinstellungen**.
4. Hier finden Sie eine Schaltfläche, die entweder **Biometrie deaktivieren** oder **Biometrie aktivieren** anzeigt. Diese Einstellung steuert den Betriebszustand der Funktion für biometrische Authentifizierung.

4.2.2. Zurücksetzen des Master-Passworts

> **Wichtig**
> Die Funktion **Master-Passwort ändern** ist auf Mobilgeräten nicht verfügbar. Sie können Ihr Master-Passwort ausschließlich über die Browser-Erweiterung Bitdefender Password Manager auf einem Windows-PC oder einem macOS-Gerät ändern oder wiederherstellen.

Gehen Sie wie folgt vor, um Ihr**Master-Passwort** als Vorsichtsmaßnahme zu ändern und ein neues Master-Passwort im Bitdefender Password Manager festzulegen:.

1. Klicken Sie nach Installation der Browsererweiterung auf das **Password Manager**-Symbol in der Symbolleiste Ihres Browsers.
2. Geben Sie Ihr aktuelles Master-Passwort ein, um den Tresor zu entsperren.

   > **Wichtig**
   > Falls Sie Ihr aktuelles Master-Passwort vergessen haben, klicken Sie auf diesem Bildschirm stattdessen auf die Option **Ich habe mein Passwort vergessen**. Geben Sie den **24-stelligen Wiederherstellungsschlüssel** ein, den Sie bei der Ersteinrichtung Ihres Bitdefender Password Managers erhalten haben. Geben Sie danach ein neues Master-Passwort ein. **Falls Sie** sowohl Ihr **Master-Passwort** als auch den **Wiederherstellungsschlüssel** vergessen oder verlegt haben, wenden Sie sich **als letzte Option an einen Bitdefender-Mitarbeiter, um Hilfe beim Zurücksetzen Ihres Kontos zu erhalten**. Beim Zurücksetzen Ihres Kontos werden **alle in Bitdefender Password Manager gespeicherten Daten und Passwörter gelöscht**.

3. Öffnen Sie das Password Manager-Menü , um die Seitenleiste auf der linken Seite zu erweitern, und klicken Sie auf **Einstellungen** Menüpunkt.
4. Klicken Sie im Abschnitt **Konto** auf **Mein Konto**.
5. Ein Fenster mit Informationen zu Ihrem Password Manager-Abonnement wird angezeigt.
   Klicken Sie auf **Master-Passwort ändern**.
6. Sie werden zu einem neuen Fenster weitergeleitet, in dem Sie ein neues Master-Passwort festlegen können. Geben Sie zunächst Ihr aktuelles Master-Kennwort und danach das neue Master-Passwort ein. Das neue Master-Kennwort muss mindestens 8 Zeichen lang sein und mindestens einen Kleinbuchstaben, einen Großbuchstaben und eine Zahl enthalten.
7. Klicken Sie im Anschluss auf **Ändern**.
8. Warten Sie einen Moment, bis Bitdefender das alte Master-Passwort zurückgesetzt hat.
   Schließen Sie Ihren Webbrowser nicht!
9. Im nächsten Schritt erhalten Sie einen neuen **24-stelligen Wiederherstellungsschlüssel**. Bewahren Sie Ihren

Wiederherstellungsschlüssel an einem sicheren Ort auf und **verlieren Sie ihn nicht**. Dieser Schlüssel ist die einzige Möglichkeit, auf Ihre im Password Manager gespeicherten Passwörter zuzugreifen, sollten Sie Ihr Master-Passwort vergessen.
Klicken Sie im Anschluss auf **Schließen**.

10. Sie werden von Bitdefender Password Manager abgemeldet.
Geben Sie zum Entsperren des Tresors das neue Master-Passwort ein, das Sie gerade festgelegt haben.

4.3. Weitere Funktionen

4.3.1. Verwaltung von Identitäten

Mit dieser Funktion können Benutzer mehrere Identitäten speichern und mit dem Password Manager ihre Daten in Webformularen automatisch ausfüllen. So wird Online-Shopping schnell, einfach und sicher.

Wie alles andere im Password Manager sind auch die sensiblen Daten, die zu diesen gespeicherten Identitäten gehören, verschlüsselt und nur auf dem Gerät des Benutzers abrufbar.

So können Sie im Password Manager eine Identität hinzufügen:

1. Klicken Sie unter Windows oder macOS auf die **Password Manager** Symbol in Ihrem Webbrowser.
Starten Sie unter Android oder iOS die **Password Manager** Anwendung.
Wenn Sie dazu aufgefordert werden, geben Sie Ihre ein Master Passwort.
2. Öffnen Sie das Passwort Manager-Menü, um die Menüleiste links einzublenden und klicken Sie auf den Menüpunkt **Einstellungen**.
3. Klicken Sie unten auf **Identität hinzufügen**.
4. Geben Sie die Daten ein, die gespeichert werden sollen, und klicken Sie auf **Speichern**.

4.3.2. Verwalten von Kreditkarten

Mit dieser Funktion können Sie Ihre Kreditkartendaten speichern und automatisch eingeben, um einfacher, schneller und sicherer einzukaufen.

So können Sie im Password Manager eine Kreditkarte hinzufügen:

1. Klicken Sie unter Windows oder macOS auf die **Password Manager** Symbol in Ihrem Webbrowser.
   Starten Sie unter Android oder iOS die **Password Manager** Anwendung.
   Wenn Sie dazu aufgefordert werden, geben Sie Ihre ein Master Passwort.
2. Öffnen Sie das Passwort Manager-Menü, um die Menüleiste links einzublenden und klicken Sie auf den Menüpunkt **Kreditkarten**.
3. Drücken Sie auf die **Identität hinzufügen** Knopf unten.
4. Vervollständigen Sie die Details, die Sie speichern möchten, und drücken Sie dann **Speichern**.

4.3.3. Meine Absicherung

Mit der Funktion Meine Absicherung können Sie sich jederzeit per Fernzugriff abmelden und Ihren Browserverlauf auf Ihrem Computer, Tablet oder Mobilgerät löschen. Wir empfehlen diese Funktion besonders dann, wenn Sie Ihr Gerät nicht alleine nutzen.

So finden und aktivieren Sie diese Funktion:

1. Klicken Sie unter Windows oder macOS auf die **Password Manager** Symbol in Ihrem Webbrowser.
   Starten Sie unter Android oder iOS die **Password Manager** Anwendung.
   Wenn Sie dazu aufgefordert werden, geben Sie Ihre ein Master Passwort.
2. Öffnen Sie das Passwort Manager-Menü, um die Menüleiste links einzublenden und klicken Sie auf den Menüpunkt **Meine Absicherung**.
3. Klicken Sie auf **Alle Sitzungen absichern**.
   Wenn Sie nur ein einzelnes Gerät absichern möchten, suchen Sie es in der Liste der Geräte, auf denen der Password Manager installiert oder im Browser aktiviert ist.

4.3.4. Notizen

Die Funktion Sichere Notizen ist Ihr geheimes Notizbuch, in dem Sie vertrauliche Informationen speichern, ordnen und zur besseren Übersicht

farblich kennzeichnen können. So sind die Informationen nicht nur gut organisiert, sondern auch sicher und vor fremden Zugriff geschützt.

So finden und aktivieren Sie diese Funktion:

1. Klicken Sie unter Windows oder macOS auf die **Password Manager** Symbol in Ihrem Webbrowser.
   Starten Sie unter Android oder iOS die **Password Manager** Anwendung.
   Wenn Sie dazu aufgefordert werden, geben Sie Ihre ein Master Passwort.
2. Öffnen Sie das Passwort Manager-Menü, um die Menüleiste links einzublenden und klicken Sie auf den Menüpunkt **Notizen**.
3. Klicken Sie auf **Notiz hinzufügen**.
   Geben Sie die Informationen ein, die Sie sicher aufbewahren möchten, und klicken Sie auf **Speichern**.

5. HÄUFIG GESTELLTE FRAGEN

Es gibt Fragen zum Bitdefender Password Manager, die uns immer wieder begegnen. Die passenden Antworten haben wir an dieser Stelle für Sie zusammengestellt. Hier erfahren Sie alles Wissenswerte über Ihr Bitdefender-Konto, den Import von Passwörtern, unsere Datensicherheitsprotokolle und andere wichtige Themen, die unsere Kunden beschäftigen.

Allgemeine Fragen zum Bitdefender Password Manager

Wie werde ich das Password Manager-Pop-up in meiner Bitdefender-Sicherheitslösung los?

Die Password Manager-Benachrichtigung, die in Bitdefender Total Security, Internet Security und Antivirus Plus angezeigt wird, können Sie durch Klicken auf die Schaltfläche "x" schließen. Das Fenster "Verwalten Sie Ihre Passwörter mit dem Bitdefender Password Manager" erscheint zufällig ein paar Mal, wird danach aber nicht wieder angezeigt. Sie können diese Werbemitteilung abstellen, indem Sie die **Benachrichtigungen zu Empfehlungen** in den Bitdefender-Einstellungen auf "Aus" stellen.

Was passiert, wenn mein Bitdefender Password Manager-Abonnement abläuft?

Wenn Ihr Password Manager-Abonnement abläuft und nicht mehr aktiv ist, haben Sie maximal 90 Tage Zeit, um Ihre Passwörter zu exportieren. Ihre Passwörter werden für weitere 30 Tage als Sicherungskopie gespeichert. Während dieser 90 Tage können Sie Ihre Daten nur exportieren. Sie können den Password Manager nicht weiter verwenden. Die Funktion zum automatischen Ausfüllen von Passwörtern funktioniert dann nicht mehr, ebenso wie die Möglichkeit, neue Passwörter zu generieren.

Nach Ablauf der 90-tägigen Frist haben Sie weitere 30 Tage Zeit, um den Bitdefender-Support zu kontaktieren und die Wiederherstellung Ihrer Passwörter in der Live-Datenbank zu veranlassen. Sie können dann Ihre Passwörter aus dem Bitdefender Password Manager exportieren.

Ihre Daten werden in der Live-Datenbank nur bis zum Ende des Tages aufbewahrt, an dem Sie Ihre Anfrage auf Wiederherstellung gestellt

haben. Um Mitternacht wird die Datenbank gelöscht - falls Sie die 30-tägige Nachfrist noch nicht überschritten haben, können die Passwörter aus der Sicherungskopie erneut wiederhergestellt werden. Die gesicherten Rohdaten in der Datenbank können dem Benutzer auf Anfrage zur Verfügung gestellt werden, die Datenbank ist jedoch verschlüsselt und die Informationen sind nicht zugänglich.

Was ist ein Master-Passwort, und warum muss ich es mir merken?

Das Master-Passwort ist der Schlüssel, der die Tür zu allen in Ihrem Bitdefender Password Manager-Konto gespeicherten Passwörtern öffnet. Das Master-Passwort muss mindestens 8 Zeichen lang sein. Erstellen Sie also ein starkes Master-Passwort, merken Sie es sich gut und geben Sie es niemals an Dritte weiter. Um ein starkes Master-Passwort zu erstellen, empfehlen wir Ihnen, eine Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen (z. B. #, $ oder @) zu verwenden.

Wie verhindere ich, dass Bitdefender mich bei jedem Öffnen des Browsers nach meinem Master-Passwort fragt?

Wenn Sie Ihr Gerät sperren, ohne den Browser zu schließen, wird der Password Manager nicht gesperrt und Sie können nach Ihrer Rückkehr sofort auf Ihre Daten zugreifen. Als Sicherheitsmaßnahme müssen Sie sich jedoch bei jedem erneuten Öffnen des Browsers mit Ihrem Bitdefender Central-Konto anmelden und dann Ihr Master-Passwort eingeben.

- Um die Aufforderung zur Anmeldung bei Central zu deaktivieren, rufen Sie die ⚙ Einstellungen auf und aktivieren Sie die Option "Anmeldereiter beim Start deaktivieren".
- Um die Aufforderung zur Eingabe des Master-Passworts zu deaktivieren, markieren Sie die Option "Meine Anmeldedaten speichern" im Fenster "Ihren Tresor entsperren".

Warum wird mein Master-Passwort nicht gespeichert und was passiert, wenn ich es vergesse?

Wir speichern Ihr Master-Passwort nicht auf unseren Servern, damit nur Sie auf Ihr Konto zugreifen können. Das gewährleistet maximale Sicherheit. Wenn der Bitdefender Password Manager Ihr Master-Passwort nicht erkennt, vergewissern Sie sich, dass Sie es richtig eingegeben haben und die Feststelltaste auf der Tastatur nicht aktiviert ist.

Falls Sie das Master-Passwort vergessen, können Sie jederzeit Ihren Wiederherstellungsschlüssel nutzen, um den Password Manager zu

entsperren. Bei der ersten Anmeldung erhalten Sie vom Bitdefender Password Manager einen **Wiederherstellungsschlüssel**, mit dem Sie den Zugang zu Ihrem Konto wiederherstellen können, ohne Ihre Daten zu verlieren.

Falls Sie sowohl das Master-Passwort als auch den Wiederherstellungsschlüssel vergessen oder verlegt haben, können Sie sich als letzte Option an einen Bitdefender-Mitarbeiter wenden, um Ihr Konto zurücksetzen zu lassen.

> **Wichtig**
> Beim Zurücksetzen Ihres Kontos werden alle im Bitdefender Password Manager gespeicherten Daten und Passwörter gelöscht.

Können sich mehrere Benutzer ein Bitdefender Password Manager-Abonnement teilen?

Aktuell ist es nicht möglich, dass mehrere Benutzer ein Password Manager-Abonnement nutzen. Aber wir arbeiten daran, diese Möglichkeit in naher Zukunft bereitzustellen.

Was ist der Offlinemodus und wie funktioniert er?

Der Offlinemodus wird automatisch aktiviert, wenn Ihre Internetverbindung während der Nutzung des Bitdefender Password Managers unterbrochen wird. Wenn Sie bereits angemeldet sind und Ihr Master-Passwort eingegeben haben, können Sie im Offline-Modus auch dann auf Ihre Passwörter zugreifen, wenn keine Internetverbindung verfügbar ist.

Wie kann ich den Bitdefender Password Manager deinstallieren?

Gehen Sie zur Deinstallation des Bitdefender Password Managers wie folgt vor:

- Unter Windows und macOS:
  Entfernen Sie die Password Manager-Erweiterung aus Ihrem Webbrowser. Klicken Sie mit der rechten Maustaste auf das Bitdefender-Symbol und wählen Sie "Entfernen".
- Android:
  Tippen Sie auf die Password Manager-App und halten Sie sie gedrückt. Ziehen Sie sie dann an den oberen Rand des Bildschirms zum Menüpunkt "Deinstallieren".
- Unter iOS und iPadOS:

Tippen Sie auf die Password Manager-App und halten Sie sie gedrückt, bis alle Apps auf Ihrem Bildschirm zu wackeln beginnen. Tippen Sie jetzt auf das X oben links neben dem Bitdefender-Symbol.

Datenschutz- und Sicherheitsfragen rund um den Bitdefender Password Manager

Können Bitdefender-Mitarbeiter meine Passwörter einsehen?

Auf keinen Fall. Der Schutz Ihrer Daten hat für uns oberste Priorität. Das ist auch der wichtigste Grund, warum wir Ihr Master-Passwort nicht auf unseren Datenservern speichern: Damit niemand außer Ihnen Zugang zu Ihrem Konto hat, nicht einmal die Mitarbeiter unseres Unternehmens. Jedes Passwort und jedes Konto sind mit dem stärksten Datensicherheitsalgorithmus hochgradig verschlüsselt. Der uns angezeigte Code erscheint lediglich als eine zufällig zusammengewürfelte Folge von Zahlen und Buchstaben.

Was würde bei einem Hack der Password Manager-Server passieren?

Jedes Passwort wird lokal auf Ihrem Gerät verschlüsselt, bevor es überhaupt in die Nähe unserer Server gelangt. Sollten Hacker also in unser System eindringen, würden sie nur Seiten mit zufälligen Folgen aus Buchstaben und Zahlen sehen, ohne Ihren Schlüssel, um sie zu entschlüsseln. Das bedeutet, dass Sie und Ihre Kontodaten bei uns jederzeit sicher sind.

6. HILFE UND SUPPORT

6.1. Hier wird Ihnen geholfen

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

6.2. Online-Ressourcen

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

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

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

6.2.1. Bitdefender-Support-Center

Das Bitdefender-Support-Center ist eine Online-Sammlung von Informationen zu Ihren Bitdefender-Produkten. Hier sind in einem leicht zugänglichen Format Berichte zu den Ergebnissen des fortlaufenden technischen Supports sowie der Bugfix-Aktivitäten der Bitdefender-Support- und Entwicklungsteams gespeichert. Hinzu kommen Artikel zur Bedrohungsvorbeugung, detaillierte Erklärungen zur Verwaltung von Bitdefender-Lösungen und vieles mehr.

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

Grundlagen und Fachwissen über unsere Produkte zu erlangen. Alle 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/.

6.2.2. Die Bitdefender Experten Community

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

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

Hier geht's zur Website unserer Expert Community:

https://community.bitdefender.com/de

6.2.3. Bitdefender Cyberpedia

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

Die Bitdefender Cyberpedia finden Sie hier:

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

6.3. Kontaktinformation

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

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

6.3.1. Lokale Vertriebspartner

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

So finden Sie einen Bitdefender Distributor in Ihrem Land:

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

GLOSSAR

Aktivierungscode

Dabei handelt es sich um einen eindeutigen Schlüssel, der käuflich erworben und zur Aktivierung eines Produkts oder eines Dienstes verwendet werden kann. Mit einem Aktivierungscode kann ein gültiges Abonnement für einen bestimmten Zeitraum und eine bestimmte Anzahl an Geräten aktiviert werden. Zudem kann mit einem solchen Code eine Abonnement verlängert werden, solange es sich auf das gleiche Produkt oder den gleichen Dienst bezieht.

ActiveX

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