BENUTZERHANDBUCH

Bitdefender CONSUMER SOLUTIONS

SecurePass

Bitdefender SecurePass

Bedienungsanleitung

Publication date 20/11/2024

Impressum

Bitdefender

Inhaltsverzeichnis

ÜBER DIESE ANLEITUNG

Zielsetzung und Zielgruppe

Dieses Bitdefender SecurePassHandbuch 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 SecurePass.

Import und Export Ihrer Passwörter (Seite 11)

Erfahren Sie, wie Sie Passwörter in und aus SecurePass importieren oder exportieren können.

Funktionen und Merkmale (Seite 15)

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

Hilfe und Support (Seite 28)

Hinweise zu nützlichen Informationen und Hilfestellungen bei unerwarteten Problemen.

Konventionen in diesem Handbuch

Typografie

Um die Lesbarkeit zu fördern werden verschiedene Arten von Textstilen verwendet. Die jeweiligen Bedeutungen entnehmen Sie bitte der nachfolgenden Tabelle.

Erscheinungsbild	Beschreibung
Beispielsyntax	Syntaxbeispiele sind in Konstantschrift dargestellt.
https://www.bitdefender.com	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 sind in Konstantschrift dargestellt.
Optionen	Alle Produktoptionen sing **fett** gedruckt.
Stichwort	Wichtige Stichwörter oder Ausdrücke werden durch **fett** hervorgehoben.

Zusätzliche Hinweise

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

Hinweis

Ein solcher Hinweis ist nur eine Anmerkung. Sie können ihn überspringen, dennoch können Hinweise auch nützliche Informationen z. B. zu einzelnen Funktionen oder verwandten Themen liefern.

Wichtig

Diese Art von Hinweis sollte in jedem Fall gelesen werden. Es handelt sich in der Regel nicht kritische, aber dennoch wichtige Informationen.

Warnung

Hierbei handelt es sich um kritische Informationen, die besondere Vorsicht erfordern. Hier angegebenen Anweisungen und Informationen sollten Sie auf jeden Fall Beachtung schenken. Sie müssen unbedingt gelesen und verstanden werden, weil sie auf riskante Vorgänge hinweisen.

Ihre Mithilfe

Wir laden Sie ein mit zu helfen unser Buch zu verbessern. Wir haben sämtliche Informationen in diesem Dokument bestmöglich überprüft um somit die Qualität sicherzustellen. Bitte schreiben Sie uns bezüglich Fehler, die in diesem Buch finden oder auch bezüglich Dinge, die Ihrer Meinung nach verbessert werden könnten. Dies hilft uns Ihnen die beste mögliche Dokumentation zur Verfügung zu stellen.

Schicken Sie Ihre Anmerkungen an documentation@bitdefender.com. Bitte verfassen Sie bitte alle auf die Dokumentation bezogenen E-Mails auf Englisch, damit wir sie schnellstmöglich bearbeiten können.

1. WAS IST BITDEFENDER SECUREPASS

Bitdefender SecurePass 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 SecurePass 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. 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 SecurePass nur auf Geräten mit den folgenden Betriebssystemen nutzen:

- **Für PC-Benutzer:**
  - Windows 7 mit Service Pack 1
  - 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 SecurePass 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 SecurePass-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**.

- **Google Chrome**
- **Mozilla Firefox**

- **Microsoft Edge**
- **Safari**

So installieren Sie Bitdefender SecurePass:

1. Folgen Sie nach dem Kauf von Bitdefender SecurePass den Anweisungen in der Bestätigungs-E-Mail, um Ihr Abonnement zu aktivieren.
2. Melden Sie sich mit Ihren Zugangsdaten bei Bitdefender Central an. Wählen Sie im Menü auf der linken Seite **SecurePass**.
3. Wählen Sie im SecurePass-Panel Ihren bevorzugten Browser aus.
4. Installieren Sie die Browsererweiterung:
   - **Google Chrome:**
     a. Klicken Sie auf **Zu Chrome hinzufügen** Schaltfläche.
     b. Klicken Sie im Bestätigungsfeld auf **Erweiterung hinzufügen**.
   - **Mozilla Firefox:**
     a. Klicken Sie auf **Zu Firefox hinzufügen** Knopf.
     b. Klicken Sie auf **Installieren** Schaltfläche in der oberen rechten Ecke des Bildschirms.
   - **Microsoft Edge:**
     a. Klicken Sie auf **Holen** Knopf.
     b. klicken **Erweiterung hinzufügen** in der angezeigten Eingabeaufforderung.
   - **Safarifahrt:**
     a. Das SecurePass-Installationsprogramm wird auf Ihr macOS-Gerät heruntergeladen. Doppelklicken Sie auf die heruntergeladene Datei und folgen Sie von dort aus den Anweisungen auf dem Bildschirm
     b. Öffnen Sie am Ende des Installationsvorgangs die **Safari** Browser und wählen **Einstellungen** in der oberen Menüleiste.
     c. Klicken Sie in den Einstellungsfenstern auf **Registerkarte „Erweiterungen“**.

d. Markieren Sie das Kästchen neben **Bitdefender SecurePass** um es zu aktivieren.

Sobald die Erweiterung installiert ist, können Sie mit dem Einrichtungsvorgang (Seite 9).

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.

1. Öffnen Sie nach dem Kauf vor allem die Bestätigungs-E-Mail, die Sie erhalten haben, um den dortigen Anweisungen zur Aktivierung Ihres SecurePass-Abonnements zu folgen.
2. Öffnen Sie den Google Play Store auf Ihrem Android-Gerät.
3. Geben Sie in der Suchleiste des Google Play Store Folgendes ein **Bitdefender SecurePass**, suchen Sie die Anwendung und laden Sie sie herunter.
4. Sobald der Download abgeschlossen ist, öffnen Sie die App und folgen Sie bei Bedarf den Konfigurationsschritten auf dem Bildschirm, die erforderlich sind, um den Installationsvorgang abzuschließen.

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.

1. Öffnen Sie nach dem Kauf vor allem die Bestätigungs-E-Mail, die Sie erhalten haben, um den dortigen Anweisungen zur Aktivierung Ihres SecurePass-Abonnements zu folgen.
2. Öffnen Sie den App Store auf Ihrem iOS-Gerät.
3. Geben Sie in der Suchleiste des App Store Folgendes ein **Bitdefender SecurePass**, suchen Sie die Anwendung und laden Sie sie herunter.

4. Sobald der Download abgeschlossen ist, öffnen Sie die App und folgen Sie bei Bedarf den Konfigurationsschritten auf dem Bildschirm, die erforderlich sind, um den Installationsvorgang abzuschließen.

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

2.3. Einrichtungsvorgang

So richten Sie Bitdefender SecurePass auf Ihrem Browser/Mobilgerät ein:

1. Öffnen Sie nach Abschluss des Installationsvorgangs die SecurePass-Erweiterung/Anwendung und melden Sie sich an.
   Verwenden Sie die Anmeldedaten des Bitdefender-Kontos, das mit Ihrem SecurePass-Abonnement verknüpft ist.
2. Sie werden aufgefordert, eine zu erstellen **Master-Passwort**.

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

   Achten Sie darauf, ein sicheres Master-Passwort einzugeben, ohne das Risiko einzugehen, es leicht zu vergessen.
   Sobald Sie sich für ein sicheres und einzigartiges Master-Passwort entschieden haben, klicken Sie auf **Speichern und fortfahren**.
3. Als Nächstes erhalten Sie eine **Wiederherstellungsschlüssel**.

   Warnung
   Nach der Erstellung 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 im Password Manager gespeicherten Passwörter zuzugreifen, falls Sie **vergessen Sie das Master-Passwort** zuvor für Ihr Konto eingerichtet.

   - Speichern Sie den Wiederherstellungsschlüssel, indem Sie ihn in Ihre Zwischenablage kopieren oder als PDF-Datei herunterladen.
     Du kannst drücken **Schliessen** wenn fertig.

4. Wenn Sie fertig sind, wählen Sie die **Greife auf deinen Vault zu** Schaltfläche.

Nachdem der Einrichtungsvorgang abgeschlossen ist, können Sie mit der Nutzung von Bitdefender SecurePass beginnen.

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:

- Bitdefender Passwort-Manager
- Bitdefender-Brieftasche
- Bitdefender SecurePass
- Sicherer Pass
- 1Passwort
- Kaspersky
- Dashlane
- Chrome-Browser
- Firefox-Browser
- Microsoft Edge
- Bitwächter
- LastPass
- Keepass
- RoboForm

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. Öffnen Sie Bitdefender SecurePass und gehen Sie zu **Einstellungen**.
   - Im Browser:
     Klicken Sie auf **Einstellungen** in der oberen rechten Ecke der Seite.
   - In der App:
     Tippe auf **Mehr** klicken Sie in der unteren rechten Ecke des Bildschirms und tippen Sie oben in der Liste, die anschließend erscheint, auf **Einstellungen**.
2. In der **Sichern und Wiederherstellen** Abschnitt, wählen **Passwörter importieren**. Das Importfenster wird geöffnet.
3. Wählen Sie den Namen des Passwort-Managers oder Web-Browsers, den Sie zuvor verwendet haben, aus dem Drop-down-Menü aus, auf das Sie über **Wählen Sie den Dateityp** Feld.

   > **Hinweis**
   > Wenn ein Passwort verwendet wurde, um die Datei zu verschlüsseln, müssen Sie es in das **Passwort** Feld; andernfalls können Sie es leer lassen.

4. Wählen Sie die **Wählen Sie die zu importierende Datei aus** eingereicht.
   Navigieren Sie zu dem Ort, an dem die exportierten Daten Ihres alten Passwort-Managers gespeichert wurden. Wählen Sie die Datei aus, sobald Sie sie gefunden haben, und klicken Sie dann auf **Öffnen**.
5. Nachdem Sie die Datei ausgewählt haben, wählen Sie **Importieren** in der unteren linken Ecke des Importfensters. Der Vorgang beginnt in Kürze und wird von einer Fortschrittsanzeige begleitet

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

> **Hinweis**
> Wenn Sie in SecurePass zu Ihrem Passwort-Tresor zurückkehren, werden Sie einen Ordner mit dem Namen sehen **Importieren**, das alle Daten aus Ihrem vorherigen Passwort-Manager oder Webbrowser enthält.

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. Öffnen Sie Bitdefender SecurePass und gehen Sie zu **Einstellungen**.
   - Im Browser:
     Klicken Sie auf **Einstellungen** in der oberen rechten Ecke der Seite.
   - In der App:
     Tippe auf **Mehr** klicken Sie in der unteren rechten Ecke des Bildschirms und tippen Sie oben in der Liste, die anschließend erscheint, auf **Einstellungen**.
2. In der **Sichern und Wiederherstellen** Abschnitt, wählen **Passwörter exportieren**. Das Exportfenster wird geöffnet.
3. Klicken Sie auf **Wählen Sie den Dateityp**. Wählen Sie im Dropdownmenü aus, ob Sie Ihre Daten entweder im JSON-Format oder im CSV-Format exportieren möchten. Sie können auch ein

Passwort eingeben, mit dem die exportierte Datei geschützt werden soll.
Markieren Sie das entsprechende Kästchen, wenn Sie auch geteilte Elemente einbeziehen möchten.

4. klicken **Exportieren** in der unteren linken Ecke des Exportfensters und speichern Sie die exportierte Datei auf Ihrem Gerät.

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. Passwörter manuell speichern

Sie können Informationen wie Passwörter, Anmeldeinformationen und andere Informationen wie Kreditkarteninformationen oder Notizen manuell auf folgende Weise sicher in Bitdefender SecurePass speichern:

1. Öffnen Sie Bitdefender SecurePass
2. In der **Mein Tresor** Drücken Sie die Tabulatortaste **+Artikel hinzufügen** Schaltfläche.
3. Wählen Sie den Artikeltyp aus, den Sie hinzufügen möchten. (Konto, Kreditkarte, Identität oder Notiz).
4. Füllen Sie je nach ausgewähltem Artikel die erforderlichen Felder aus.
5. Nachdem Sie alle erforderlichen Angaben gemacht haben, speichern Sie den Artikel, um ihn zu Ihrem SecurePass-Tresor hinzuzufügen.

4.2. Passwort-Generator

Bitdefender SecurePass enthält eine Funktion zur Passwortgenerierung, die bei der Erstellung sicherer Passwörter helfen kann.

So greifen Sie auf den Passwortgenerator zu und verwenden ihn:

1. Öffnen Sie Bitdefender SecurePass und greifen Sie auf den **Passwort generieren** Tab auf der linken Seite des Bildschirms. Dadurch gelangen Sie zum Passwortgenerator, der in SecurePass integriert
2. Passen Sie das Passwort, das Sie generieren möchten, an Ihre eigenen Bedürfnisse und Vorlieben an.
   - Passwortlänge: Ziehen Sie den Schieberegler, um eine beliebige Länge zwischen 8 und 32 Zeichen festzulegen.
   - Groß-/Kleinbuchstaben: Wählen Sie aus, welche oder beide Buchstabentypen Sie für die Komplexität Ihres Passworts hinzufügen möchten.

- Zahlen: Wenn Sie dieses Kästchen ankreuzen, werden Zahlen in die Zeichenfolge aufgenommen, aus der Ihr Passwort besteht.
- Sonderzeichen: Fügen Sie Ihrem Passwort Symbole hinzu, um die Komplexität des Passworts zu erhöhen.

> **Hinweis**
> Drücken Sie die **Speichern Sie die Einstellungen** Schaltfläche, damit SecurePass sie sich merkt und Passwörter immer auf der Grundlage der von Ihnen gespeicherten Einstellungen generiert.

3. Generieren Sie ein neues Passwort, indem Sie auf das kreisförmige Pfeilsymbol unter dem aktuell angezeigten Passwort klicken. Bei jedem Klick wird eine neue Zeichenfolge generiert.
4. Wenn Sie mit dem generierten Passwort zufrieden sind, können Sie es entweder in Ihre Zwischenablage kopieren oder auf das **Konto speichern** Schaltfläche, um es in Ihrem Tresor zu speichern (durch Verknüpfung mit anderen Kontoinformationen).

> **Hinweis**
> Sie können auch schnell ein Passwort generieren **direkt aus den Anmeldeformularen** indem Sie auf das Bitdefender SecurePass-Symbol im Passwortfeld der Anmeldeseite klicken. Wenn Sie darauf klicken, können Sie dann das auswählen **Passwort generieren** Option.

4.3. Überprüfung der Passwortstärke

Bitdefender SecurePass bietet die Möglichkeit, die Stärke von gespeicherten Passwörtern und sensiblen Daten zu bewerten. Dies ist eine wichtige Funktion bei der Bewertung und Bewertung potenzieller Sicherheitslücken in Bezug auf Ihren Datenschutz und Ihre Sicherheit

Um die Stärke der gespeicherten Passwörter zu überprüfen:

1. Öffnen Sie Bitdefender SecurePass und wählen Sie im E-Mail-Menü den **Sicherheitsbericht** Tab.
   Die Registerkarte „Sicherheitsbericht“ ist in vier Abschnitte unterteilt: Sicherheitslücken, Schwächen, Alte und Duplikate.
2. Die Anzahl der Passwörter, die in jede der vier Kategorien fallen, wird auf dem Bildschirm angezeigt.

Wenn Sie die Liste der gespeicherten Passwörter durchgehen, wird jedes Passwort zusätzlich mit der Kategorie gekennzeichnet, unter der es sich befindet.

Um die Bedeutung dieser Sicherheitsstufen zu verstehen, finden Sie im Folgenden einige kurze Informationen zu den einzelnen Sicherheitsstufen:

- Verletzte Passwörter: Wenn einer Ihrer Zugangsdaten Teil einer Datenschutzverletzung war, werden sie unter dem **verletzt** Abschnitt.

  > **Hinweis**
  > Um zu überprüfen, ob eines Ihrer Passwörter kompromittiert wurde und durch Datenschutzverletzungen durchgesickert ist, klicken Sie auf **Führen Sie den Sicherheitsscan durch** Knopf.

- Schwache Passwörter: SecurePass identifiziert und kennzeichnet **schwach** Passwörter, die in Ihrem Tresor gespeichert werden, basieren auf einem internen, lokal laufenden Algorithmus, der unter anderem verschiedene Kriterien wie die Länge des Passworts, die Anzahl der Zeichen und die Einbeziehung von Ziffern oder Großbuchstaben berücksichtigt.
- Alte Passwörter: Passwörter, die für einen längeren Zeitraum als sechs Monate gespeichert und unverändert gespeichert wurden, werden als gekennzeichnet **alt**.
- Doppelte Passwörter: Da die Verwendung derselben Passwörter auf mehreren Plattformen und Konten ein großes Sicherheitsrisiko darstellt, kennzeichnet SecurePass Passwörter, die an mehr als einer Stelle verwendet werden, als **duplizieren**.

4.4. Organisation der Daten

In Bitdefender SecurePass können Sie all Ihre gespeicherten Artikel organisieren und somit einfacher verwalten.

Sie können Ihre Artikel für einen einfachen Zugriff in bestimmte Ordner kategorisieren, indem Sie die folgenden Schritte ausführen:

1. Öffnen Sie Bitdefender SecurePass und gehen Sie zu **Mein Tresor**. Tippen Sie hier auf **Ordner hinzufügen** Schaltfläche.
2. Benennen Sie Ihren Ordner und tippen Sie auf **Erstellen** Schaltfläche. Der neue Ordner wird jetzt in Ihrem Tresor angezeigt.

Um Elemente in Ihren erstellten Ordner zu verschieben:

1. Klicken Sie auf ein Konto, das Sie verschieben möchten, und drücken Sie die **Bearbeiten** Schaltfläche.
2. Drücken Sie auf den neben angezeigten Ort **Artikel speichern in** und wählen Sie den Ordnernamen aus der Dropdownliste aus.
3. Drücken Sie die **Konto speichern** Schaltfläche.

Das Konto wird jetzt im ausgewählten Ordner gespeichert.

4.5. Intelligentes automatisches Ausfüllen

Mit Bitdefender SecurePass können Sie Kontodaten und Informationen in allen Online-Anmeldeformularen automatisch ausfüllen.

> **Hinweis**
> Als Webbrowser-Erweiterung sollte die AutoFill-Funktion unter Windows oder macOS problemlos funktionieren.

4.5.1. Automatisches Ausfüllen auf Android

So konfigurieren Sie SecurePass auf Android, um Autofill zu verwenden:

1. Öffnen Sie die Bitdefender SecurePass-App auf Ihrem Android-Gerät.
2. Tippe auf **Mehr** Menü-Schaltfläche.
3. Tippen Sie oben auf dem Bildschirm auf **Einstellungen**.
4. Tippe auf **Machen Sie dies zu Ihrem Standard-Passwort-Manager**
5. Aktivieren Sie Bitdefender SecurePass in der AutoFill-Serviceliste.

> **Hinweis**
> Sie können auch zu den Einstellungen Ihres Android-Geräts gehen, in **Passwörter und Konten** > **Dienst zum automatischen Ausfüllen** > Bitdefender SecurePass aktivieren.
>
> Für Android 11 oder frühere Versionen des Betriebssystems lauten die Einstellungen: **System** > **Sprache und Eingabe** > **Fortgeschritten**.

6. Tippen Sie **OK**.

Sobald diese Konfiguration abgeschlossen ist, erscheint jedes Mal, wenn Sie auf ein Anmeldefeld tippen, eine Option namens Bitdefender

SecurePass auf Ihrem Bildschirm. Sie können darauf tippen, um die App zu öffnen. Melden Sie sich bei SecurePass an und Ihre Anmeldeinformationen werden automatisch eingegeben

4.5.2. Automatisches Ausfüllen auf iOS

So konfigurieren Sie SecurePass auf Ihrem iOS-Gerät, um Autofill zu verwenden:

1. Öffne das **Einstellung** App auf Ihrem iPhone oder iPad und wählen Sie **Allgemein**.
2. Tippe auf **Automatisches Ausfüllen und Passwörter**. Stellen Sie die Option **Passwörter und Kennwörter automatisch ausfüllen** oder **Passwörter automatisch ausfüllen** - abhängig von der iOS-Version - ist aktiviert.
3. In der **Formular automatisch ausfüllen** Liste, aktiviere die **Bitdefender SecurePass** Anwendung.

Sobald diese Konfiguration abgeschlossen ist, erscheint jedes Mal, wenn Sie auf ein Anmeldefeld tippen, eine Option namens Bitdefender SecurePass auf Ihrem Bildschirm. Sie können darauf tippen, um die App zu öffnen. Melden Sie sich bei SecurePass an und Ihre Anmeldeinformationen werden automatisch eingegeben

4.5.3. Kartendetails automatisch ausfüllen

Während SecurePass ein leicht zugängliches Symbol zum automatischen Ausfüllen von Anmeldedaten und Passwörtern bietet, funktioniert die AutoFill-Funktion für Kreditkarteninformationen anders:

1. Navigieren Sie zur Zahlungs- oder Checkout-Seite der Website, auf der Sie Ihre gespeicherten Kreditkarteninformationen verwenden möchten.
2. Klicken Sie mit der rechten Maustaste auf einen leeren Bereich der Zahlungsseite. Dadurch wird das Kontextmenü auf Ihrem Bildschirm angezeigt
3. Wählen Sie Bitdefender SecurePass aus dem Menü aus, indem Sie den Mauszeiger über die Option bewegen. Dadurch wird ein Untermenü mit weiteren Optionen geöffnet

4. Wählen Sie die **Kreditkarteninformationen automatisch ausfüllen**. Daraufhin wird eine Liste aller Kreditkarten angezeigt, die Sie im SecurePass-Tresor gespeichert haben
5. Wählen Sie die bevorzugte Karte aus.

Auf diese Weise füllt SecurePass die Felder des Zahlungsformulars automatisch mit den Daten der von Ihnen ausgewählten Kreditkarte aus.

5. ALS 2FA-ANWENDUNG VERWENDEN

Sie können Bitdefender SecurePass jederzeit als App zur zweistufigen Authentifizierung für jede beliebige Website oder Plattform verwenden und Ihre 2FA-Codes zusammen mit Ihren Passwörtern wie folgt verwalten:

1. Gehen Sie zu den Sicherheitseinstellungen der Website oder Anwendung, auf der Sie die 2FA-Funktion aktivieren möchten. In der Regel wird Ihnen während des Vorgangs ein QR-Code oder ein Bestätigungscode angezeigt
2. Starten Sie Bitdefender SecurePass und greifen Sie auf das entsprechende Konto zu, das Sie für die 2FA-Nutzung konfigurieren möchten. Klicken Sie auf **Bearbeiten** Schaltfläche.
3. Scrollen Sie in SecurePass auf der Kontoeintragsseite zum Ende und drücken Sie auf **Zwei-Faktor-Authentifizierung** Option.
4. Scannen Sie den QR-Code oder geben Sie den Code manuell ein.
   Sobald dies geschehen ist, bestätigt SecurePass die erfolgreiche Einrichtung der Zwei-Faktor-Authentifizierung.
5. Danach drücken Sie die neue **Code anzeigen** Schaltfläche jetzt in der Oberfläche sichtbar. Dort wird ein zeitkritischer Code angezeigt
6. Kehren Sie zu dem Konto zurück, in dem Sie die 2FA-Funktion aktiviert haben, und geben Sie den Code von Bitdefender SecurePass ein, um Ihre Einrichtung zu überprüfen.

Drücken Sie nach Abschluss dieses Einrichtungsvorgangs die **Konto speichern** Schaltfläche in SecurePass, um den Vorgang abzuschließen.

Wenn Sie sich von nun an auf der Plattform anmelden, für die Sie die 2FA-Funktion eingerichtet haben, werden Sie aufgefordert, die 2FA-Codes von SecurePass für das jeweilige Konto zu verwenden, was eine neue Sicherheitsebene für das betreffende Konto bietet.

6. DATEN TEILEN

Bitdefender SecurePass bietet die Möglichkeit, vertrauliche Informationen wie Anmeldeinformationen, Passwörter oder Kreditkartendaten sicher weiterzugeben.

Sie können die Sharing-Funktion über Links verwenden:

1. Wählen Sie einen Artikel aus, der in Ihrem Tresor gespeichert ist.
   - Im Browser:
     Gehe zu deinem Tresor und klicke auf den Artikel, den du teilen möchtest. Klicken Sie auf der rechten Seite auf das Drei-Punkte-Menü und wählen Sie **Link teilen**.
   - In der App:
     Gehe zu deinem Tresor und tippe auf das Objekt, das du teilen möchtest. Tippe auf das Linksymbol und wähle **Link zum Teilen generieren** Option.
2. Erstellen Sie den Link Teilen, indem Sie Folgendes angeben:
   - Das Ablaufdatum des Links.
   - Das Nutzungslimit.
   - Ob der Link passwortgeschützt sein soll oder nicht.
3. Kopieren Sie den generierten Link nach der Generierung und senden Sie ihn an den gewünschten Empfänger.

6.1. Mit Gruppen teilen

Gruppen werden erstellt, um den Datenaustausch noch einfacher zu gestalten. Sie können innerhalb von Bitdefender SecurePass verschiedene Gruppen mit anderen Benutzern erstellen, um vertrauliche Daten sicher auszutauschen

1. Eine Gruppe erstellen:
   - Gehe zu **Gruppen** und drücken Sie **Gruppe erstellen** Schaltfläche auf der Registerkarte Gruppen.
   - Geben Sie einen Gruppennamen ein und drücken Sie dann die **Gruppe erstellen** Schaltfläche.

2. Artikel zu Gruppen hinzufügen:
   - Im Browser:
     Gehe zu deinem Tresor und klicke auf den Artikel, den du teilen möchtest. Klicke auf das Drei-Punkte-Menü auf der rechten Seite des Elements und wähle **Zur Gruppe hinzufügen**.
   - In der App:
     Gehe zu deinem Tresor und klicke auf den Artikel, den du teilen möchtest. Wählen Sie das **Mit der Gruppe teilen** Option.

   Wählen Sie die Gruppe aus, mit der Sie das Element teilen möchten.
3. Legen Sie die Zugriffsrechte (Lesen, Schreiben, Gewähren) auf der Grundlage des Kontrollniveaus fest, das Sie den Gruppenmitgliedern gewähren möchten.
4. Drücken **Speichern**, dann **Erledigt**.

Du und die Gruppenmitglieder können geteilte Elemente im Gruppenbereich überprüfen.

6.2. Gruppen verwalten

In der **Gruppen** Im Bitdefender SecurePass-Bereich können Sie alle erstellten Gruppen einsehen und sie nach Ihren Bedürfnissen verwalten:

- Benennen Sie Gruppen um.
- Mitglieder bearbeiten. (neue Mitglieder einladen, bestimmten Mitgliedern Rechte zuweisen, Admin- oder Sharing-Rechte gewähren und bestehende Mitglieder entfernen)
- Gruppen verlassen.
- Gruppen löschen.

7. KONTO SPERREN

Bitdefender SecurePass wird mit einem **Konto sperren** Funktion, die Ihr Konto sofort sperrt und alle aktiven Sitzungen auf allen Geräten beendet, die Zugriff darauf haben. Diese Funktion ist besonders praktisch, wenn der Verdacht eines unbefugten Zugriffs besteht

So sperren Sie Ihr SecurePass-Konto:

1. Öffnen Sie Bitdefender SecurePass.
2. Einmal in SecurePass:
   - Im Browser:
     Klicken Sie auf **Einstellungen** in der oberen rechten Ecke der Seite.
   - In der mobilen App:
     Tippe auf **Sichere mich** Menütaste.
3. Drücken Sie die **Konto sperren** Taste, um sich sofort von allen Geräten abzumelden und laufende Sitzungen zu beenden.

8. 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

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.

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.

Was ist der Offline-Modus?

Der Offline-Modus wird automatisch aktiviert, wenn die Internetverbindung während der Verwendung von Bitdefender SecurePass unterbrochen wird. Wenn Sie bereits angemeldet sind und Ihr Master-Passwort eingegeben haben, können Sie im Offline-Modus 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.

9. HILFE UND SUPPORT

9.1. Hier wird Ihnen geholfen

Bitdefender bietet seinen Kunden konkurrenzlos schnellen und kompetenten Support. Sollten sich Probleme ergeben oder Sie eine Frage zu Ihrem Bitdefender-Produkt haben, so stehen Ihnen verschiedene Online-Quellen zur Verfügung, wo Sie Lösungen und Antworten finden.

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/support/consumer.html.

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, Datenschutzverletzungen, Identitätsdiebstahl und Social-Media-Identitätsbetrug 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. Rufen Sie https://www.bitdefender.com/partners/partner-locator.html</link> auf.
2. Geben Sie über die entsprechenden Optionen Ihren Wohnort und Ihr Land an.

GLOSSAR

Aktivierungs-Code

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

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 Administrator absichtlich hinterlässt. Der Grund dafür muss nicht immer bösartig sein. Manche Betriebssysteme haben schon standardmäßig privilegierte Konten eingerichtet, damit diese von den Kundendienst-Technikern oder Programmierern der Hersteller benutzt werden können.

Boot-Sektor

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.

Botnetz

Das Wort "Botnetz" setzt sich aus Bestandteilen der Wörter "Roboter" und "Netzwerk" zusammen. Bei Botnetzen handelt es sich um Netzwerke 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.

Ereignisanzeige

Ereignisse oder Erscheinungen, die in einem Programm vorkommen. Ereignisse können Benutzeraktionen, wie zum Beispiel Mausklicks oder Tastatureingaben, oder Systemereignisse, wie zum Beispiel ungenügender Speicher, sein.

Exploits

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

Falsch Positiv

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

Dateierweiterungen

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 und 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.

Heuristisch

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.

Honigtopf

Ein Computersystem, das als Köder dient, um Hacker anzulocken und danach ihr Verhalten zu beobachten. Daraus lassen sich Schlüsse ziehen, mit welchen Methoden Sie Daten sammeln. Besonders Unternehmen und Konzerne setzen auf den Einsatz dieser "Honigtöpfe", um ihren Sicherheitslage zu verbessern.

IP

Internet Protocol - Das TCP/IP Protokoll ist verantwortlich für die korrekte IP Adressierung und die korrekte Zustellung der Datenpakete.

Java-Applet

Ein Java Programm, das nur auf Webseiten läuft. Um ein Applet auf einer Webseite zu benutzen, gibt man den Namen und die Größe (Länge und Breite in Pixel) an, die das Applet einnehmen kann. Wenn die Webseite abgerufen wird, lädt der Browser das Applet vom Server herunter und führt es auf der Benutzermaschine (dem Client) aus. Applets sind keine Anwendungen, da sie von strengen Sicherheitsprotokollen gesteuert werden.

Obwohl Applets z. B. auf dem Client laufen, können diese keine Daten auf der Maschine des Clients lesen oder schreiben. Zusätzlich sind die Applets dahingehend beschränkt, dass sie nur Daten aus der Domain lesen und schreiben können, zu der sie gehören.

Keylogger

Ein Keylogger ist eine Anwendung, die alle Ihre Tastenanschläge aufzeichnet. Keylogger sind an sich nicht schädlich. Sie können auch legitim eingesetzt werden, um beispielsweise die Aktivitäten von Angestellten oder Kindern zu überwachen. Sie werden jedoch zunehmend von Cyber-Kriminellen mit 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.

E-Mail-Client

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

Speicher

Interne Speicherbereiche im Rechner. Der Begriff Arbeitsspeicher bezeichnet Datenträger in Form von sehr schnellen Chips. Dies steht im Gegensatz zu Speicherplatz, der sich auf Magnetbändern

oder Datenträgern befindet. Jeder Rechner hat eine gewisse Menge Arbeitsspeicher. Dieser wird auch Hauptspeicher oder RAM bezeichnet.

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-Missbrauchstäter

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.

Gepackte Programme

Eine Datei in einem komprimierten Format. Viele Betriebssysteme und Anwendungen enthalten Befehle, mit denen Dateien komprimiert werden können, so dass diese weniger Speicherplatz benötigen. Zum Beispiel: Angenommen, Sie haben einen Text, der 10 aufeinander folgende Leerzeichen enthält. Normalerweise belegen diese Leerzeichen dann 10 Bytes an Speicherplatz.

Ein Programm, das Dateien komprimiert, würde die Leerzeichen durch ein Sonderzeichen „Leerzeichenreihe“ ersetzen, gefolgt von der Zahl der Leerzeichen, die ersetzt wurden. In diesem Fall sind nur noch zwei Bytes notwendig statt zehn. Das wäre ein Beispiel für eine Komprimierungstechnik, es gibt aber noch viele andere.

Pfad

Zeigt die Stelle an, an der sich eine Datei in einem Rechner befindet. Diese Pfadangaben enthalten gewöhnlich den hierarchischen Aufbau des Dateiverzeichnisses: Laufwerke, Ordner, Unterverzeichnisse, die Datei und ihre Erweiterung.

Der Weg zwischen zwei Punkten, wie zum Beispiel der Kommunikationskanal zwischen zwei Rechnern.

Phishing

Das Senden einer E-Mail an einen Benutzer, in der der Sender sich als Vertreter eines legitimen Unternehmens ausgibt und versucht, den Empfänger so zu manipulieren, dass er persönliche Informationen

preisgibt, die dann zum Diebstahl der Identität verwendet werden können. Die E-Mail leitet den Benutzer dann auf eine Webseite, auf der er aufgefordert wird, vertrauliche Daten wie Kreditkartennummern, TANs oder PINs preiszugeben. Es wird oft vorgegeben, dass dies aus Gründen der Aktualisierung geschehen soll. Diese Webseiten sind jedoch gefälscht und wurden eigens für den Diebstahl dieser Daten eingerichtet.

Photon

Photon ist eine innovative und unaufdringliche Bitdefender-Technologie, die eigens entwickelt wurde, um die Auswirkungen der Sicherheitslösung auf die Systemleistung zu minimieren. Durch die Hintergrundüberwachung aller PC-Aktivitäten werden Nutzungsprofile erstellt, mit denen Start- und Scan-Prozesse optimiert werden können.

Polymorphes 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.

Schnittstelle

Stelle eines Rechners, an die ein Gerät angeschlossen werden kann. Rechner haben verschiedenartige Schnittstellen. Im Inneren gibt es Schnittstellen zum Anschluss von Festplatten, Grafikkarten und Tastaturen. Extern haben Rechner Schnittstellen zum Anschluss von Modems, Druckern und anderen Peripheriegeräten.

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

Ransomware

Bei Ransomware handelt es sich um schädliche Programme, die anfällige Systeme für den Benutzer sperren und für deren Freigabe Lösegeld erpressen. CryptoLocker, CryptoWall und TeslaWall sind nur einige Beispiele für Ransomware, die es auf Benutzercomputer abgesehen haben.

Die Infektion kann sich durch das Aufrufen 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 Prokolldatei mit den geprüften Pfaden, Ordnern, der Anzahl der gescannten Archive und Dateien sowie der Anzahl der gefundenen infizierten oder verdächtigen Dateien.

Rootkit

Bei einem Rootkit handelt es sich um eine Sammlung von Software-Tools, mit denen auf ein System mit Administratorrechten zugegriffen werden kann. Der Begriff wurde ursprünglich nur für UNIX-Systeme verwendet und beschrieb rekompilierte Tools, mit denen sich Angreifer Administratorrechte verschaffen und so ihre Anwesenheit vor den tatsächlichen Administratoren verbergen konnten.

Die Hauptaufgabe eines Rootkits besteht darin, Prozesse, Dateien und Protokolle zu verstecken. Sie können auch Daten von Terminals, Netzwerkverbindungen oder Peripheriegeräten abfangen, falls Sie eine entsprechende Software eingebaut haben.

Rootkits sind nicht grundsätzlich schädlich. Einige Systeme und Anwendungen verstecken z. B. wichtige Dateien mithilfe von Rootkits. Sie werden jedoch oft dazu missbraucht, Bedrohungen zu verbergen oder unbemerkt einen Eindringling einzuschleusen. In Kombination mit anderen Bedrohungen stellen Rootkits eine große Gefahr für Ihr System dar. Denn sie können den Datenverkehr abhören, Sicherheitslücken in Ihrem System schaffen, Dateien und Zugangsdaten verändern, und das alles, ohne entdeckt zu werden.

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-Postings in Newsgroups. Im Allgemeinen versteht man darunter jede Art von unerwünschter E-Mail.

Spyware

Software, die unentdeckt vom Nutzer private und geheime Anwenderdaten über seine Internetverbindung abgreift. Dies geschieht in der Regel zu Werbezwecken. Typischerweise sind Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Shareware-Programmen

enthalten, die aus dem Internet heruntergeladen werden können. Die große Mehrzahl von Shareware- und Freeware-Anwendungen ist natürlich frei von Spyware. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an einen Dritten. Spyware kann auch Informationen über E-Mail-Adressen und sogar Passwörter und Kreditkartennummern sammeln.

Einer Bedrohung durch ein trojanisches Pferd ähnelt Spyware darin, dass die Anwender das Produkt unwissentlich gemeinsam mit etwas anderem installieren. Opfer von Spyware wird man oft dann, wenn man sich bestimmte Peer-to-Peer-Dateiaustauschprogramme herunterlädt.

Ganz abgesehen von den Fragen der Ethik und des Datenschutzes belegt Spyware auch unnötig Systemressourcen und Bandbreite, indem über die Internetverbindung des Nutzers Informationen an den Spyware-Heimatserver gesendet werden. Da Spyware Speicher und Systemressourcen verbraucht, können die im Hintergrund laufenden Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.

Startup Objekt (Autostart-Objekt)

Jede Datei, die sich in diesem Ordner befindet, wird geöffnet, wenn der Rechner gestartet wird. Das können z. B. ein Startbildschirm, eine Sounddatei, die beim Systemstart abgespielt wird, ein Erinnerungskalender oder auch Apps sein. Gewöhnlich wird eine Alias-Datei (Verknüpfung) statt der eigentlichen Datei in diesen Ordner gelegt.

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.

Infobereich

Die Symbolleiste wurde mit Windows 95 eingeführt und befindet sich auf der Windows Task-Leiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet). Sie enthält kleine Symbole zur Information und zum leichteren Zugriff auf Systemfunktionen wie Drucker, Modems, Lautstärke und anderes. Um auf die Details und Optionen dieser Funktionen zuzugreifen, ist ein Doppelklick oder ein Klick mit der rechten Maustaste erforderlich.

TCP/IP

Transmission Control Protocol/Internet Protocol – im Internet weit verbreiteter Netzwerkprotokollsatz, der die Kommunikation zwischen verbundenen Computernetzwerken mit verschiedenen Hardware-Architekturen und Betriebssystemen ermöglicht. TCP/IP bietet eine Möglichkeit, all diese unterschiedlichen Komponenten zu Kommunikationszwecken miteinander zu verbinden.

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 Homers "Ilias", in der die Griechen ihren Feinden, den Trojanern, angeblich als Sühnegabe ein riesiges hölzernes Pferd schenkten. Aber nachdem die Trojaner das Pferd in die Stadt gebracht hatten, schlichen sich die im Bauch des hölzernen Pferdes versteckten Soldaten bei Nacht heraus, öffneten die Tore der Stadt und ermöglichten somit ihren Landsleuten, in die Stadt einzudringen und auf diese Weise Troja zu besetzen.

Update (Aktualisierung)

Eine neue Software- oder Hardwareversion, die eine ältere Version desselben Produkts ersetzt. Die Update-Installationsroutine eines Programms prüft oft, ob eine ältere Versionen auf dem Rechner installiert ist, da sonst kein Update installiert werden kann.

Bitdefender verfügt über eine eigene Update-Funktion, über die Sie manuell nach Updates suchen oder das Produkt automatisch aktualisieren lassen können.

Virtual Private Network (VPN)

Mit dieser Technologie ist es möglich, eine zeitlich begrenzte und verschlüsselte direkte Verbindung mit einem bestimmten Netzwerk auch über ein weniger gut gesichertes Netzwerk aufzubauen. Auf diese Weise können Daten sicher und verschlüsselt versandt und empfangen werden und sind für neugierige Augen nur schwer einsehbar. Bei einem Sicherheitsnachweis handelt es sich um eine Authentifizierung, die ausschließlich über einen Benutzernamen und ein Passwort erfolgen kann.

Wurm

Ein Programm, das sich selbst kopiert und über ein Netzwerk verbreitet. Es kann sich nicht an andere Programme anhängen.