BENUTZERHANDBUCH

Bitdefender CONSUMER SOLUTIONS

Parental Control

Bitdefender Parental Control

Benutzerhandbuch

Publication date 04/29/2024

Rechtlicher Hinweis

Bitdefender

Inhaltsverzeichnis

ÜBER DIESE ANLEITUNG

Zielsetzung und Zielgruppe

Dieses Benutzerhandbuch richtet sich an alle Bitdefender-Benutzer, die sich für die Bitdefender-Kindersicherung als Lösung für die Sicherheit, die Überwachung und den kontinuierlichen Schutz der Geräte und der Online-Präsenz ihrer Kinder entschieden haben.

Sie erfahren, wie Sie Bitdefender Kindersicherung installieren, konfigurieren und optimal einsetzen, um auch von den erweiterten Funktionen zu profitieren und die Online-Aktivitäten Ihrer Kinder jederzeit im Griff zu haben.

Viel Spaß mit diesen nützlichen und informativen Handbuch.

Über dieses Handbuch

Dieses Handbuch behandelt die folgenden Themengebiete:

Erste Schritte (Seite 4)

Erste Schritte zur Einrichten Ihrer Bitdefender-Kindersicherung.

Funktionen und Merkmale (Seite 10)

Der richtige Umgang mit der Bitdefender-Kindersicherung und ihren Funktionen.

Hilfe und Support (Seite 23)

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.
<link xlink:href="urn:resource:component:28104">Über diese Anleitung</link>	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. ERSTE SCHRITTE

Wir beginnen mit einer detaillierten, schrittweisen Anleitung, wie Sie das Abonnement der Bitdefender-Kindersicherung in Ihrem Bitdefender Central-Benutzerkonto einrichten. Dies ist der erste Schritt in einem einfachen Prozess, der es Ihnen ermöglicht, die Online-Aktivitäten Ihrer Kinder effektiv zu verwalten und zu überwachen.

1.1. Einrichten der Kindersicherung

Nach der Aktivierung Ihres Abonnements können Sie die Bitdefender-Kindersicherung über Ihr Konto einrichten:

1. Rufen Sie Ihr Bitdefender Central-Konto auf und öffnen Sie den Reiter **Kindersicherung** links auf dem Bildschirm.
2. Klicken Sie auf **Erste Schritte**.
3. Legen Sie eine PIN für die App fest.

   > **Hinweis**
   > Dieser PIN-Code verhindert, dass Ihre Kinder die Funktionen der Kindersicherung deaktivieren, indem sie sich aus ihrer Kinder-App ausloggen.
   >
   > Merken Sie sich unbedingt diese PIN.

4. Klicken Sie auf **Weiter**.
5. Erstellen Sie ein Profil für Ihr Kind. Geben Sie den Namen des Kindes ein und wählen Sie ein Profilbild aus. Klicken Sie dann auf **Weiter**.
6. Wählen Sie das Alter Ihres Kindes aus. Klicken Sie anschließend auf **Weiter**.
7. Geben Sie an, ob die App zur Kindersicherung auf dem gerade genutzten Gerät oder auf einem weiteren Gerät installiert werden soll.

Hinweis

Wenn Sie **Weitere Geräte** auswählen, stehen Ihnen drei Installationsoptionen zur Verfügung. Wählen Sie die gewünschte Option aus:

- QR-Code scannen.
- Bereitgestellten Link kopieren und im Browser auf dem Gerät des Kindes öffnen.
- Den Installationslink per E-Mail versenden.

8. Warten Sie, bis der Download abgeschlossen ist, und starten Sie dann das Installationsprogramm auf dem jeweiligen Gerät.

Damit beginnt der Installationsvorgang. Die weiteren Schritte hängen vom Gerätetyp und dem Betriebssystem ab, auf dem die Installation durchgeführt wird.

1.2. Installation der Bitdefender-Kindersicherung auf den Geräten Ihrer Kinder

1.2.1. Auf Windows-Geräten:

Sobald Sie das eben heruntergeladene Installationsprogramm ausführen:

1. Klicken Sie auf **Ja**, wenn Sie in einem Dialog zur Benutzerkontensteuerung aufgefordert werden, der Installationsdatei zu erlauben, Änderungen am Gerät vorzunehmen.
2. Melden Sie sich mit den Anmeldedaten Ihres Bitdefender Central-Kontos an, wenn Sie dazu aufgefordert werden.

1.2.2. Auf macOS-Geräten:

Sobald der Download des Installationsprogramms abgeschlossen ist, doppelklicken Sie auf die Bitdefender-Datei, um den Installationsvorgang zu starten:

1. Sie werden durch die für die Installation von Bitdefender-Kindersicherung für macOS erforderlichen Schritte geführt. Klicken Sie auf **Zulassen**, wenn Sie dazu aufgefordert werden.
2. Klicken Sie auf die beiden aufeinanderfolgenden **Fortfahren**-Schaltflächen.

3. Um mit der Installation fortzufahren, müssen Sie den Bedingungen der Software-Abonnementvereinbarung zustimmen.
4. Klicke auf **Fortfahren**. Klicken Sie danach auf **Installieren**.
5. Wenn Sie dazu aufgefordert werden, geben Sie einen Administratornamen und ein Passwort ein und drücken Sie dann auf die Schaltfläche **Software installieren**.

Warten Sie, bis Sie eine Pop-up-Meldung erhalten, dass eine *Systemerweiterung blockiert* wurde. Das ist bei diesem Vorgang ganz normal. Zum Fortfahren müssen Sie die Systemerweiterung Kindersicherung wie im Folgenden beschrieben zulassen:

1. Klicken Sie auf die Schaltfläche **Systemeinstellungen öffnen**.

> **Hinweis**
> In früheren macOS-Versionen heißt diese Schaltfläche noch **Sicherheitseinstellungen öffnen**.

2. Klicken Sie in dem jetzt angezeigten Fenster auf die Schaltfläche **Zulassen** und geben Sie dann einen Administratornamen und ein Passwort ein, um die Einstellungen freizugeben.

> **Hinweis**
> Unter macOS 11 (Big Sur) und macOS 12 (Monterey) müssen Sie, bevor Sie auf die Schaltfläche **Zulassen** klicken können, zunächst auf das Vorhängeschlosssymbol links unten im Fenster **Sicherheit & Datenschutz** klicken und dann einen Administratornamen und ein Passwort eingeben, um Änderungen vorzunehmen.

3. Das Pop-up-Fenster **Netzwerkinhalte filtern** wird angezeigt. Klicken Sie in diesem Fenster auf **Zulassen**.
4. Klicken Sie danach auf die Schaltfläche **Systemeinstellungen öffnen**.
5. Klicken Sie ein weiteres Mal auf die Schaltfläche **Zulassen**.

1.2.3. Auf Android-Geräte:

Im Google Play Store öffnet sich Bitdefenders Seite für die App der Kindersicherung:

1. Tippen Sie auf die Schaltfläche **Installieren**. Die App wird nun heruntergeladen und installiert.

2. Nach Abschluss der Installation erscheint eine **Öffnen**-Schaltfläche. Tippen Sie sie an, um die App der Bitdefender-Kindersicherung zu starten.

Folgen Sie nach dem Öffnen der App den Anweisungen auf dem Bildschirm, um die Kindersicherung auf dem Android-Gerät Ihres Kindes einzurichten:

1. Tippen Sie auf **Fortfahren**.
2. Melden Sie sich mit Ihren Bitdefender Central-Anmeldedaten bei der App an.
3. Wählen Sie das Kindesprofil aus, das Sie dem Android-Gerät zuweisen möchten.
4. Sie müssen der App die erforderlichen Berechtigungen erteilen, damit sie ordnungsgemäß funktioniert. Tippen Sie dazu auf **Weiter** und gehen Sie danach wie folgt vor:
   a. Lassen Sie den VPN-Zugriff zu und wählen Sie dann **Immer zulassen**, um Online-Inhalte auf dem Gerät Ihres Kindes zu filtern.
   b. Um das Android-Gerät Ihres Kindes orten zu können, tippen Sie auf **Weiter**, dann auf **Zulassen** und wählen Sie die Option **Immer zulassen**.
   c. Die Berechtigungen für VPN und Standort werden mit einem grünen Haken angezeigt. Tippen Sie auf **Einrichtung abschließen** und danach auf **Weiter**.
   d. An dieser Stelle sind drei weitere Berechtigungen erforderlich, um den Internetzugang und Apps auf dem Gerät des Kindes zu blockieren. Tippen Sie unter **Geräteadministratorrechte** auf **Berechtigung festlegen**.
   e. Tippen Sie auf **Beenden**, wenn Sie die Einrichtung der App der Bitdefender-Kindersicherung abgeschlossen haben.

1.2.4. Auf iOS-Geräten:

Im App Store öffnet sich Bitdefenders Seite für die App der Kindersicherung:

1. Tippen Sie auf das Wolkensymbol mit dem nach unten zeigenden Pfeil. Die App wird nun heruntergeladen und installiert.

2. Nach Abschluss der Installation erscheint eine **Öffnen**-Schaltfläche. Tippen Sie sie an, um die App der Bitdefender-Kindersicherung zu starten.
3. Wenn auf dem iOS-Gerät des Kindes Mobile Device Management-Profile gefunden werden, werden Sie aufgefordert, diese zu entfernen. Tippen Sie auf **Weiter** und danach auf **Profile entfernen**.
4. Wählen Sie in der **Einstellungs-App** auf dem iOS-Gerät die Option **Allgemein**, scrollen Sie dann nach unten und tippen Sie auf den Abschnitt **VPN & Geräteverwaltung**.
5. Tippen Sie auf jeden Eintrag im Abschnitt **MOBILE DEVICE MANAGEMEN** und wählen Sie **Verwaltung löschen** für jedes Gerät.
   Wiederholen Sie diesen Vorgang, bis keine Einträge mehr unter MOBILE DEVICE MANAGEMENT vorhanden sind.

Öffnen Sie die auf dem Gerät des Kindes installierte App erneut und folgen Sie den Anweisungen auf dem Bildschirm, um die Bitdefender-Kindersicherung einzurichten:

1. Tippen Sie auf **Fortfahren**.
2. Melden Sie sich mit Ihren Bitdefender Central-Anmeldedaten bei der App an.
3. Wählen Sie das Kindesprofil aus, das Sie dem Android-Gerät zuweisen möchten.
4. Anschließend müssen Sie die erforderlichen Berechtigungen erteilen, damit die App ordnungsgemäß funktioniert. Tippen Sie auf **Weiter**.
5. Lassen Sie den VPN-Zugang zu, um Online-Inhalte auf dem Gerät Ihres Kindes zu filtern. Tippen Sie zweimal hintereinander auf **Zulassen**, um die VPN-Konfigurationen hinzuzufügen.
6. Tippen Sie auf **Weiter** und wählen Sie dann **Zulassen**, um die Ortung des iOS-Geräts Ihres Kindes zu ermöglichen.
7. Richten Sie anschließend die Apple Familienfreigabe ein, um den Internetzugang und die Apps auf dem Gerät des Kindes sperren zu können.

> **Hinweis**
> Tippen Sie auf **So geht's**, um eine schrittweise Anleitung zu erhalten.

8. Nachdem Sie die Apple Familienfreigabe auf Ihrem eigenen Gerät und auf dem Gerät Ihres Kindes konfiguriert haben, wählen Sie zum Fortfahren **Ich habe die Apple Familienfreigabe konfiguriert**.
9. Lassen Sie dann Zugriff auf Bildschirmzeit zu, um Online-Inhalte auf dem iOS-Gerät Ihres Kindes zu filtern.
10 Tippen Sie auf **Einrichtung abschließen**.

.

Nachdem Sie diese Schritte auf dem Gerät bzw. den Geräten Ihres Kindes durchgeführt haben, ist der Einrichtungsvorgang abgeschlossen. Als Elternteil können Sie ab sofort die Online-Aktivitäten Ihres Kindes überwachen und Nutzungsstatistiken in Ihrem Bitdefender Central-Konto im Dashboard Kindersicherung einsehen, auf das wir in den folgenden Kapiteln näher eingehen werden.

2. FUNKTIONEN UND MERKMALE

2.1. Profile

Ein Kindesprofil ist ein benutzerdefinierter Satz von Regeln, anhand derer die App der Bitdefender-Kindersicherung die Online-Aktivitäten eines Kindes steuern und überwachen kann. Dazu gehören z. B. Einstellungen wie Inhaltsfilter und Zeitbeschränkungen, die auf das Alter des Kindes zugeschnitten sind. Über ihr Bitdefender Central-Konto können Eltern diese Profile erstellen, bearbeiten und löschen sowie ihnen Geräte zuweisen und entfernen, um eine sichere und angemessene Internetnutzung für ihre Kinder zu gewährleisten.

So legen Sie ein Kindesprofil an:

1. Rufen Sie Bitdefender Central auf und melden Sie sich bei Ihrem Konto an.
2. Klicken Sie im Menü links auf den Reiter **Kindersicherung**.
3. Klicken Sie auf **Neues Profil**, um ein neues Kindesprofil zu erstellen.
4. Geben Sie den Namen, das Profilbild und das Geburtsdatum des Kindes ein.

   > **Hinweis**
   > Je nach Alter des Kindes blockiert Bitdefender automatisch bestimmte Kategorien wie Chats, soziale Netzwerke, nicht jugendfreie Inhalte und vieles mehr. Sie können später eigene Anpassungen an den blockierten Kategorien vornehmen.

5. Klicken Sie auf **Speichern**.

Das neue Profil wird angelegt und auf der Seite angezeigt.

So bearbeiten Sie ein Kindesprofil:

1. Klicken Sie im Profil des Kindes auf **Details anzeigen**.
2. Unter **Profil editieren** können Sie Änderungen am Profil Ihres Kindes vornehmen.
3. Nutzen Sie das entsprechende Feld, um den Namen, den Geburtstag und/oder das Profilbild des Kindes zu ändern.

4. Klicken Sie nach der Änderung der erforderlichen Angaben auf **Änderungen speichern**.

So löschen Sie das Profil eines Kindes:

1. Klicken Sie im Profil des Kindes auf **Details anzeigen**.
2. Wählen Sie **Profil editieren**.
3. Klicken Sie auf **Profil löschen** und bestätigen Sie den Löschvorgang.

So weisen Sie dem Profil eines Kindes Geräte zu:

Wenn Ihr Kind mehrere Geräte hat (Windows, macOS, Android oder iOS), können Sie sie demselben Kindesprofil zuweisen.

1. Klicken Sie im Profil des Kindes auf **Details anzeigen**.
2. Klicken Sie auf die Anzahl der Geräte, die unter seinem Namen aufgeführt sind.
3. Klicken Sie auf **Gerät zuweisen**.
4. Wählen Sie den Gerätenamen aus und klicken Sie dann auf **Zuweisen**.

> **Hinweis**
> Wenn das Gerät in der Liste nicht erscheint, klicken Sie auf **Auf einem neuen Gerät installieren** und folgen Sie den Anweisungen auf dem Bildschirm, um die Bitdefender-Kindersicherung auf dem neuen Gerät zu installieren und einzurichten.

So entfernen Sie Geräte aus dem Profil eines Kindes:

Wenn Sie ein Gerät aus dem Profil eines Kindes entfernen, bedeutet dies, dass das Gerät nicht mehr von der Bitdefender-Kindersicherung verwaltet wird. Die im Profil des Kindes festgelegten Regeln und Einstellungen gelten dann nicht mehr für dieses Gerät. Die App der Kindersicherung bleibt zwar auf dem Gerät installiert, kann aber nicht mehr genutzt werden.

1. Klicken Sie im Profil des Kindes auf **Details anzeigen**.
2. Klicken Sie auf die Anzahl der Geräte, die unter seinem Namen aufgeführt sind.
3. Suchen Sie das Gerät des Kindes und klicken Sie auf die Option **Zuweisung aufheben**.

4. Bestätigen Sie den Vorgang mit einem Klick auf **Ja, Zuweisung aufheben**.

2.2. Statistiken

Die Kindersicherung gibt Ihnen Aufschluss darüber, wie Ihre Kinder das Internet und ihre Geräte nutzen. In diesem Handbuch gehen wir auf die verschiedenen Statistiken ein, die Eltern in Bitdefender Central zur Verfügung stehen. Sie helfen Ihnen, fundierte Entscheidungen zu treffen und ein sicheres und ausgewogenes Online-Erlebnis für Ihre Kinder zu gewährleisten.

So greifen Sie auf die Statistiken zu:

1. Rufen Sie Bitdefender Central auf und melden Sie sich bei Ihrem Konto an.
2. Klicken Sie nach dem Einloggen links im Menü auf den Reiter **Kindersicherung**.
3. Klicken Sie auf das Profil des Kindes, dessen Statistiken Sie anzeigen möchten.

Nach Auswahl des Profils werden Sie zu einem Dashboard weitergeleitet, das verschiedene Statistiken anzeigt. Diese beziehen sich auf verschiedene Funktionen, die im Folgenden noch beschrieben werden.

2.3. Eltern-PIN

Die Eltern-PIN ist eine Sicherheitsfunktion im Bitdefender Central-Dashboard der Kindersicherung. Sie verhindert, dass Kinder ohne Wissen der Eltern auf die auf ihren Geräten installierte App der Kindersicherung zugreifen. Im Folgenden finden Sie eine ausführliche Anleitung, wie Sie Ihre Eltern-PIN einrichten, finden und verwalten können.

Die Eltern-PIN verhindert ein unbefugtes Abmelden von der App der Bitdefender-Kindersicherung auf dem Gerät Ihres Kindes. Bei dem Versuch, sich abzumelden, wird Ihr Kind zur Eingabe der PIN aufgefordert. So wird sichergestellt, dass nur Sie als Elternteil mit Zugriff auf das Bitdefender Central-Konto die Einstellungen der App kontrollieren können.

> **Hinweis**
> Bei der Ersteinrichtung der Kindersicherungs-App werden Sie aufgefordert, eine 4- bis 8-stellige Eltern-PIN einzugeben.

2.3.1. PIN vergessen?

Sollten Sie Ihre Eltern-PIN vergessen, können Sie sie ganz einfach über Ihr Bitdefender Central-Konto abrufen:

1. Rufen Sie Bitdefender Central auf und melden Sie sich bei Ihrem Konto an.
2. Klicken Sie nach dem Einloggen links im Menü auf den Reiter **Kindersicherung**.
3. Klicken Sie oben rechts auf der Seite auf **PIN**.
4. Klicken Sie auf das Augensymbol, um Ihren Eltern-Code anzuzeigen.

2.3.2. Ändern Ihrer PIN

Wenn Sie vermuten, dass Ihre PIN nicht mehr geheim ist, oder wenn Sie sie einfach aus Sicherheitsgründen aktualisieren möchten:

1. Klicken Sie in Ihrem Bitdefender Central-Konto im Abschnitt Kindersicherung auf die Option **PIN**.
2. Wählen Sie die Option **PIN ändern** und folgen Sie den Anweisungen auf Ihrem Bildschirm, um eine neue PIN festzulegen.

2.4. Inhaltsfilterung

Mit dem Inhaltsfilter können Eltern den Zugang ihrer Kinder zu Online-Inhalten einschränken, indem sie ganze Kategorien von Websites blockieren oder Ausnahmen für bestimmte URLs oder Themen festlegen.

> **Hinweis**
> Der Inhaltsfilter der Bitdefender-Kindersicherung hindert Kinder nicht daran, Anwendungen oder Websites offline zu nutzen, da er nur den Online-Datenverkehr der von ihnen genutzten Geräte verwaltet.

So rufen Sie den Inhaltsfilter auf:

1. Melden Sie sich bei Ihrem Bitdefender Central-Konto an.
2. Klicken Sie im Menü links auf den Reiter **Kindersicherung**.

3. Rufen Sie das Profil Ihres Kindes auf und klicken Sie oben rechts auf das Menü **Mehr**. Wählen Sie danach die Option **Inhaltsfilterung**.

2.4.1. SafeSearch und YouTube-Einschränkungen

Im Abschnitt **Privatsphäre und Sicherheit** rechts auf dem Bildschirm können Sie die Schalter Sichere Suche und YouTube eingeschränkt aktivieren.

- **Safe Search:** Bei der Nutzung von Suchmaschinen verhindert SafeSearch, dass von Google als unsicher eingestufte Ergebnisse in den Suchergebnissen angezeigt werden.
- **Eingeschränkter YouTube-Modus:** Zeigt dem Kind altersgerechte Videos auf YouTube an.

> **Hinweis**
> **SafeSearch** und der **eingeschränkte YouTube-Modus** leiten alle DNS-Anfragen von **google.com** auf **google.com** um. Die eigentliche Inhaltsfilterung erfolgt hier durch Google. Die Bitdefender-Kindersicherung filtert keine Inhalte in SafeSearch oder Google. Ebenso kann es sein, dass YouTube die Tags von Videos nicht wirksam kontrolliert, wodurch Kinder möglicherweise ungeeigneten Inhalten ausgesetzt werden.

2.4.2. Blockieren und Zulassen von Website-Kategorien

> **Hinweis**
> Im Abschnitt **Kategorien** werden die Arten von Websites, die Ihr Kind online sehen kann in Abhängigkeit von dem Alter, das bei der Erstellung des Profils des Kindes festgelegt wurde, standardmäßig zugelassen oder blockiert.

Sie können verschiedene Arten von Websites jederzeit blockieren oder zulassen:

1. Kategorie auswählen.
2. Um den Zugriff auf diese Kategorie zu blockieren, wählen Sie **Blockiert** aus dem Dropdown-Menü. Um den Zugriff zuzulassen, wählen Sie **Zugelassen**.

Wichtig

Wenn Sie die Kategorie **Filesharing** für das Profil Ihres Kindes blockieren, werden macOS-Updates nicht funktionieren. Wir empfehlen, das Filesharing bei macOS-Updates vorübergehend zuzulassen.

2.4.3. Ausnahmen

Im Reiter **Ausnahmen** können Website- und Anwendungsausnahmen festgelegt werden:

- **Website-Ausnahmen:**
  1. Klicken Sie auf **Ausnahme hinzufügen**.
  2. Wählen Sie **Nur Website** und klicken Sie dann auf **Weiter**.
  3. Geben Sie die Adresse der Website ein und wählen Sie aus dem Dropdown-Menü aus, ob sie zugelassen oder blockiert werden soll.
  4. Klicken Sie danach auf **Hinzufügen**.

- **App- und Online-Plattform-Ausnahmen:**
  1. Klicken Sie auf **Ausnahme hinzufügen**.
  2. Wählen Sie **App und Web-Plattform** und klicken Sie danach auf **Weiter**.
  3. Wählen Sie aus der Liste die Plattform aus, für die Sie eine Ausnahme festlegen möchten. Alternativ können Sie auch die Suchleiste verwenden.
  4. Klicken Sie danach auf **Hinzufügen**.

- **Ausnahmen entfernen:**
  Alle Ausnahmen, die Sie festlegen, erscheinen in der Inhaltsfilterung am unteren Rand der entsprechenden Liste.
  Um eine Ausnahme zu löschen, klicken Sie einfach auf das Papierkorbsymbol rechts neben dem Eintrag.

2.5. Tägliche Online-Zeit

In Ihrem Bitdefender Central-Konto wird im Abschnitt Kindersicherung für jedes erstellte Kindesprofil eine Karte für die tägliche Internetzeit angezeigt. Auf dieser Karte finden Sie die Gesamtzeit, die das Kind auf

allen zugewiesenen Geräten online verbracht hat. So können Sie die Online-Zeit eines Kindes einschränken:

1. Rufen Sie das Profil des Kindes auf und klicken Sie im Abschnitt **Tägliche Online-Zeit** auf **Zeitlimit festlegen**. Alternativ können Sie oben rechts auf das Menü **Mehr** klicken und **Tägliche Online-Zeit** auswählen.
2. Klicken Sie auf **Zeitlimits aktivieren**, um diese Funktion zu aktivieren.

> **Hinweis**
> Dem Kind werden standardmäßig 1 Stunde und 30 Minuten Internetzugang pro Tag zugewiesen. Wenn Eltern dieses Zeitlimit nicht verlängern, wird der Internetzugang des Kindes nach Erreichen der 1 Stunde und 30 Minuten unterbrochen.

Entfernen des täglichen Zeitlimits:

- Um die Funktion Tägliche Online-Zeit zu deaktivieren, rufen Sie das Profil Ihres Kindes auf, klicken Sie im Abschnitt **Tägliche Online-Zeit** auf **Zeit bearbeiten** und dann im Abschnitt **Zeitlimit** auf **Pause**.
- Um das Zeitlimit für einen bestimmten Tag aufzuheben, klicken Sie auf die Schaltfläche ⊗ für diesen Wochentag im Abschnitt **Zeitplan**.

Zeitlimit ändern:

- Um ein anderes Zeitlimit für einen bestimmten Wochentag festzulegen, klicken Sie im Abschnitt **Zeitplan** auf den Tag, wählen das gewünschte Limit aus dem Dropdown-Menü und klicken dann auf **Änderungen speichern**. Sie können mehrere Tage auf einmal auswählen.

2.5.1. Belohnungssystem

Mit der **Belohnungsfunktion** können Sie Ihr Kind mit mehr Bildschirmzeit belohnen oder diese verlängern und so gesunde Online-Gewohnheiten fördern. Sie können das Belohnungssystem auf zwei Arten nutzen:

- **Manuelle Belohnung:**
  1. Öffnen Sie den Abschnitt Kindersicherung in Ihrem Bitdefender Central-Konto.
  2. Rufen Sie das Profil des Kindes auf und klicken Sie im Abschnitt **Tägliche Online-Zeit** auf **Belohnen**.

3. Legen Sie die zusätzliche Zeit fest, die Sie hinzufügen möchten, und bestätigen Sie die Auswahl mit einem Klick auf **Belohnen**.

- **Nach Anfrage des Kindes:**
  Wenn Ihr Kind das Tageslimit erreicht hat, kann es über die auf seinem Mobilgerät installierte Kindersicherungs-App zusätzliche Zeit anfragen. Als Elternteil erhalten Sie eine Benachrichtigung in Ihrem Bitdefender Central-Konto.

  1. Wenn Sie in Ihrem Bitdefender Central-Konto angemeldet sind, erkennen Sie an dem roten Punkt auf der Benachrichtigungsglocke oben rechts, dass eine Anfrage Ihres Kindes aussteht.
  2. Prüfen Sie den Anfrage und entscheiden Sie, wie viel zusätzliche Zeit Sie gewähren wollen.

  > **Hinweis**
  > Kinder haben nur auf Android- und iOS-Geräten die Möglichkeit, eine Verlängerung ihrer täglichen Online-Zeit zu beantragen.

2.6. Deaktivieren des Internets auf den Geräten Ihres Kindes

Als Elternteil kann es für das Wohlergehen und die Produktivität Ihres Kindes wichtig sein, seine Internetnutzung zu kontrollieren. So deaktivieren Sie mit der Bitdefender-Kindersicherung vorübergehend den Internetzugang auf den Geräten Ihres Kindes:

1. Rufen Sie Bitdefender Central auf und melden Sie sich bei Ihrem Konto an.
2. Klicken Sie nach dem Einloggen links im Menü auf den Reiter **Kindersicherung**.
3. Wählen Sie **Details anzeigen** im Profil des Kindes, dessen Internet Sie deaktivieren möchten.
4. Klicken Sie oben rechts im Dashboard des Kindes auf **Internet anhalten**.

> **Hinweis**
> Der Internetzugang wird auf allen Geräten Ihres Kindes unterbrochen. Dieser Vorgang hat Vorrang vor allen bestehenden Einstellungen der Kindersicherung, wie z. B. Routinen, tägliche Zeitlimits oder zugelassene Kategorien.

5. Während der Zugang zum Internet unterbrochen ist, wird die Schaltfläche **Internet anhalten** als **Internet fortsetzen** angezeigt. Um den Internetzugang wiederherzustellen, müssen Sie lediglich auf **Internet fortsetzen** klicken.

2.7. Routinen

In der Bitdefender Kindersicherung können Sie bis zu drei verschiedene Routinen einrichten, um festzulegen, wann der Internetzugang Ihres Kindes ausgeschaltet wird. So können Sie die Online-Zeit Ihrer Kinder strukturieren, gesunde Gewohnheiten fördern, für mehr gemeinsame Familienzeit sorgen und gleichzeitig ihre Sicherheit gewährleisten. Diese Routinen sind voneinander unabhängig, d. h. Sie können ganz nach Bedarf nur eine, zwei oder alle drei aktivieren:

- **Konzentrationszeit**
  Erstellen Sie einen Zeitplan, der Zeit für Hausaufgaben, Lernen und andere Aktivitäten vorsieht.
- **Schlafenszeit**
  Nutzen Sie die Schlafenszeit-Routine, um eine Ruhezeit für Ihr Kind festzulegen.
- **Familienzeit**
  Nutzen Sie die Routine Familienzeit, um feste Zeiten z. B. für gemeinsame Mahlzeiten festzulegen.

Hinweis

Routinen und tägliche Online-Zeit:

Die Zeit, die Kinder während festgelegter Routinen online verbringen, wird nicht auf ihr tägliches Internet-Zeitlimit angerechnet. Sobald eine Routine beendet ist, setzt die Funktion Tägliche Online-Zeit die Erfassung der Internetnutzung durch das Kind fort.

Um Verwechslungen zu vermeiden, wird die Karte Tägliche Online-Zeit während einer laufenden Routine nicht im Profil-Dashboard des Kindes angezeigt, bis die Routine abgeschlossen ist. Stattdessen wird während dieser Zeit der Name der aktiven Routine angezeigt.

2.7.1. Einrichten von Routinen

So richten Sie die Routinen der Kindersicherung ein:

1. Rufen Sie Bitdefender Central auf und melden Sie sich bei Ihrem Konto an.
2. Klicken Sie im Menü links auf den Reiter **Kindersicherung**.
3. Rufen Sie das Profil des Kindes auf und wählen Sie im Menü **Mehr** die gewünschte Routine aus.
4. Klicken Sie auf **Aktivieren**, um die ausgewählte Routine zu aktivieren.
5. Daraufhin werden die Abschnitte **Zeitplan** und **Internetzugriff** angezeigt.

   - **Planen:**
     So legen Sie eine Routine für einen oder mehrere Tage in der Woche fest:

     a. Wählen Sie die gewünschten Tage aus.

     b. Wählen Sie die Start- und Endzeit der Routine aus dem Dropdown-Menü aus.

     c. Klicken Sie abschließend auf **Änderungen speichern**, um Ihre Auswahl zu bestätigen.

     Um die Routine für einen bestimmten Tag zu entfernen, klicken Sie auf die Schaltfläche ⊗ für diesen Wochentag.

   - **Internetzugriff:**
     Im Abschnitt Internetzugriff innerhalb einer Routine stehen Ihnen zwei Hauptfunktionen zur Steuerung der Online-Aktiviäten Ihrer Kinder zu bestimmten Zeiten zur Verfügung:

- **Vollständige Deaktivierung des Internetzugriffs:** Eltern können den Internetzugriff ihres Kindes während der festgelegten Routinezeit vollständig deaktivieren. Durch Ausschalten des Schalters **Internetzugriff** können die Geräte des Kindes innerhalb des festgelegten Zeitraums nicht auf das Internet zugreifen.
- **Ausgewählte Kategorien oder Websites:** Alternativ können Eltern den Internetzugriff zu den Routinezeiten erlauben, aber bestimmte Websites oder Inhaltskategorien einschränken. Wenn Sie den Schalter **Internetzugriff** betätigen, werden mit den Reitern **Kategorien** und **Ausnahmen**zwei weitere Reiter angezeigt, über die Sie auf weitere Einstellungen der Inhaltsfilterung</link> zugreifen können. (Seite 13)

2.8. Verfolgen des Standorts Ihres Kindes

Durch die Verbreitung von Smartphones und anderen Mobilgeräten ist die Verfolgen des Standorts von Kindern für viele Familien zu einem unverzichtbaren Hilfsmittel geworden. Ob nach der Schule oder bei Treffen mit Freunden – zu wissen, wo sich ihr Kind aufhält, beruhigt viele Eltern. Im Folgenden zeigen wir Ihnen Schritt für Schritt, wie Sie mit Ortungsfunktion der Bitdefender-Kindersicherung den Aufenthaltsort Ihres Kindes jederzeit nachverfolgen können.

1. Rufen Sie Bitdefender Central auf und melden Sie sich bei Ihrem Konto an.
2. Klicken Sie nach dem Einloggen links im Menü auf **Kindersicherung**.
3. Wenn Sie mehrere Kinder haben, wählen Sie **Details anzeigen** im Profil des Kindes, dessen Standort Sie verfolgen möchten.
4. Wählen Sie im Abschnitt Standort das Android- oder iOS-Gerät aus, das Sie verfolgen möchten, und klicken Sie dann auf die Schaltfläche **Orten**.

> **Hinweis**
> Die Ortungsfunktion der Bitdefender-Kindersicherung ist für Windows- und macOS-Geräte nicht verfügbar.

5. Nach einer kurzen Wartezeit zeigt eine rote Stecknadel den aktuellen Standort Ihres Kindes auf der Karte an.

> **Hinweis**
> Die Aktualisierung des Standorts erfolgt alle 20 Minuten. Wenn Sie versuchen, den Standort Ihres Kindes weniger als 20 Minuten nach der letzten Ortung zu ermitteln, kann die angezeigte Position möglicherweise nicht den aktuellen Aufenthaltsort in widerspiegeln.

3. DEINSTALLIEREN DER KINDERSICHERUNG

Deinstallation der Bitdefender-Kindersicherung auf Windows-Geräten:

1. Entfernen Sie das Gerät aus dem Profil Ihres Kindes in Bitdefender Central.
2. Öffnen Sie die Systemsteuerung auf dem betreffenden Gerät und suchen Sie die Bitdefender-Kindersicherung in der Liste **Programme und Features**.
3. Deinstallieren Sie die Bitdefender-Kindersicherung.

Deinstallation der Bitdefender-Kindersicherung auf macOS-Geräten:

1. Entfernen Sie das Gerät aus dem Profil Ihres Kindes in Bitdefender Central.
2. Öffnen Sie den **Finder** auf dem macOS-Gerät.
3. Rufen Sie Ihre Anwendungen auf und suchen Sie den Ordner Bitdefender.
4. Öffnen Sie ihn und führen Sie das **Bitdefender-Deinstallationsprogramm** aus.
5. Wählen Sie die Bitdefender-Kindersicherung aus der Liste der zu deinstallierenden Produkte aus.
6. Geben Sie Ihre Administrator-Anmeldedaten ein und warten Sie, bis die Deinstallation abgeschlossen ist.

Deinstallation der Bitdefender-Kindersicherung auf Android- und iOS-Geräten:

1. Entfernen Sie das Gerät aus dem Profil Ihres Kindes in Bitdefender Central.
2. Deinstallieren Sie die Kindersicherung von dem Mobilgerät wie jede andere App oder über den Google Play Store bzw. App Store.

4. HILFE UND SUPPORT

4.1. 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.

4.2. 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.

4.2.1. 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.

4.2.2. 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

4.2.3. 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/.

4.3. 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/

4.3.1. 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.