BENUTZERHANDBUCH

Bitdefender CONSUMER SOLUTIONS

# Digital Identity Protection

# Bitdefender Digital Identity Protection

**Bedienungsanleitung**

Veröffentlichungsdatum: 06.09.2023


## Impressum



Bitdefender

# Inhaltsverzeichnis

# ÜBER DIESE ANLEITUNG

## Zielsetzung und Zielgruppe

Dieses Handbuch richtet sich an alle Bitdefender-Benutzer, die sich für den Einsatz von Bitdefender Digital Identity Protection zum Schutz vor immer neuen Datenpannen im Internet entschieden haben. Die enthaltenen Informationen setzen keine besonderen Computerkenntnisse voraus, sondern dienen allen Benutzern als leicht verständliche und hilfreiche Anleitung.

Hier erfahren Sie, wie Sie wieder die Kontrolle über Ihre Privatsphäre im Internet übernehmen, indem Sie das Web mit Bitdefender Digital Identity Protection nach unbefugten Offenlegungen Ihrer persönlichen Daten durchsuchen, die Sicherheit Ihrer Benutzerkonten überwachen und einfache Anleitungen erhalten, um rechtzeitig geeignete Gegenmaßnahmen zu ergreifen. Wir helfen Ihnen, maximalen Nutzen aus Bitdefender zu ziehen.

Viel Spaß mit diesen nützlichen und informativen Handbuch.

## Über dieses Handbuch

Dieses Handbuch behandelt die folgenden Themengebiete:

Erste Schritte (Seite 6)

Beginnen Sie mit Bitdefender Digital Identity Protection und der Benutzeroberfläche.

Datenschutzverletzungen (Seite 11)

Lernen Sie, wie Sie Ihre digitale Identität optimal schützen können. Der erste Schritt liegt darin zu verstehen, was Datenpannen bedeuten und wie Sie sie richtig einschätzen, um dann geeignete Maßnahmen zum Schutz Ihrer Daten und Privatsphäre im Netz zu ergreifen.

Hilfe und Support (Seite 17)

Hinweise zu nützlichen Informationen und Hilfestellungen bei unerwarteten Problemen.

# Konventionen in diesem Handbuch

## Typografie

Zur Verbesserung der Lesbarkeit werden in diesem Handbuch verschiedene Textformate verwendet. Die Bedeutung der verschiedenen Formate können Sie der untenstehenden Tabelle entnehmen.

| Erscheinungsbild | Beschreibung |
|---|---|
| Beispielsyntax | Syntaxbeispiele werden in einer Schriftart mit fester Laufweite angegeben. |
| https://www.bitdefender.de | Verweise (Links) auf externe Inhalte auf HTTP- oder FTP-Servern. |
| documentation@bitdefender.com | Verweise auf E-Mail-Adressen, z. B. zur Kontaktaufnahme. |
| Über diese Anleitung (Seite 1) | Interne Verweise (Links) auf beliebige Stellen innerhalb dieses Dokuments. |
| Dateiname | Dateien und Verzeichnisse werden in einer Schriftart mit fester Laufweite angegeben. |
| **Option** | Alle Produktoptionen werden **fett gedruckt** dargestellt. |
| **Stichwort** | Wichtige Stichwörter oder Begriffe werden durch **Fettdruck** hervorgehoben. |

## Zusätzliche Hinweise

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

### Hinweis

Diese Bemerkung dient lediglich zur Überprüfung. Notizen enthalten nützliche Informationen wie zum Beispiel einen Verweis auf ein verwandtes Thema.

### Wichtig

Diese Art von Hinweis sollte in jedem Fall gelesen werden. Es werden signifikante Informationen zum jeweiligen Thema bereitgestellt. Es wird nicht empfohlen diese zu übergehen.

### Warnung

Diese kritische Information sollten Sie mit höchster Aufmerksamkeit verfolgen. Hier angegebenen Anweisungen und Informationen sollten Sie auf jeden Fall Beachtung schenken. Sie sollten diese Informationen sorgsam lesen und verstanden haben, da es sich um eine höchst prekäre Thematik handelt.

# Ihre Mithilfe

Wir laden Sie dazu ein uns bei der Verbesserung dieses Dokuments mitzuhelfen. Wir haben sämtliche Informationen in diesem Dokument bestmöglich überprüft um somit die Qualität sicherzustellen.

Schicken Sie uns Ihre E-Mail an documentation@bitdefender.com. Bitte verfassen Sie bitte alle auf die Dokumentation bezogenen E-Mails auf Englisch.

# 1. WAS IST BITDEFENDER DIGITAL IDENTITY PROTECTION

Schutz der Privatsphäre und Sicherheit im Internet stehen heutzutage im Mittelpunkt des Interesses von Internetnutzern. Und dafür gibt es viele gute Gründe. Weil es immer wieder zu größeren Datenpannen kommt, ist es unerlässlich, den Schutz und die Sicherheit Ihrer persönlich identifizierbaren Informationen (PII) zu gewährleisten.

Doch was gilt als persönlich identifizierbare Information? Ursprünglich galten vor allem sensible Daten wie der vollständige Name, die Sozialversicherungsnummer, der Führerschein, die Postanschrift oder Kreditkarteninformationen als PII. Mittlerweile fallen darunter auch weniger sensible Daten wie Postleitzahlen, IP-Adressen oder Anmeldekennung. Im Laufe der Zeit könnte Ihr digitaler Fußabdruck, d. h. die Daten, die Sie beim Surfen im Internet hinterlassen, einige dieser Informationen umfassen.

Bitdefender Digital Identity Protection ist Ihr ganz privater Weg zu mehr Freiheit im Internet, über den Sie sich die Kontrolle über Ihr digitales Leben zurückholen. Dazu benötigen Sie lediglich Ihren Namen, Ihre meistgenutzte E-Mail-Adresse und Ihre Telefonnummer. Auf Grundlage dieser Angaben suchen wir sowohl im öffentlich zugänglichen Internet als auch im Darknet nach persönlichen Informationen, die öffentlich zugänglich sind.

Im Funktionsumfang von Bitdefender Digital Identity Protection ist Folgendes enthalten:

- **Überwachung und Erkennung:** Der Dienst überwacht mehr als 100 personenbezogene Daten wie Kreditkartennummern oder Postanschrift und zeigt Ihnen alle Daten in Ihrem Online-Fußabdruck übersichtlich an.

  > **Notiz**
  > Bitdefender speichert und verarbeitet keine personenbezogenen Daten. Es werden nur Hinweise auf mögliche Datenpannen gespeichert, ohne dass dafür sensible Daten einbezogen werden.

- **Echtzeitwarnungen:** Sie erhalten Benachrichtigungen über Datenpannen und im Darknet gefundene Daten, persönliche

Informationen im öffentlich zugänglichen Internet sowie potenzielle Identitätsbetrüger in den sozialen Medien.

- **Lösungen:** Unser Dienst schlägt konkrete Maßnahmen vor, die zur Lösung von Problemen erforderlich sind, und erinnert Sie daran, wenn ein Problem nicht vollständig gelöst wurde. Sie können sich zudem anleiten lassen, wie Sie personalisierte Werbung unterbinden, Ihre Daten exportieren oder Tracking deaktivieren können.

# 2. ERSTE SCHRITTE

## 2.1. Digital Identity Protection aktivieren

Aktivieren Sie Ihr Bitdefender Digital Identity Protection-Abonnement, nachdem Ihre Bestellung aufgegeben und bezahlt wurde.

1. Öffnen Sie die Bestätigungs-E-Mail, die Sie kurz nach Abschluss Ihrer Bestellung erhalten haben, und klicken Sie auf **ERSTE SCHRITTE**.
2. Sie werden auf https://central.bitdefender.com weitergeleitet.
   Melden Sie sich bei Ihrem Bitdefender Central-Konto an. Wenn Sie noch kein Konto haben, erstellen Sie bitte eins.
3. Nach der Anmeldung wird das Abonnement automatisch mit Ihrem Central-Konto verknüpft und der Einrichtungsvorgang eingeleitet.

Alternativ:

- Rufen Sie in Central links im Fenster den Bereich **Meine Abonnements** auf und klicken Sie auf **+ Mit Code aktivieren**.
- Geben Sie den 10-stelligen Schlüssel ein, den Sie mit Ihrer Bestätigungs-E-Mail erhalten haben, und klicken Sie auf Sie **AKTIVIEREN**.
- Wählen Sie nach Aufforderung aus, wie Sie den Code verwenden möchten, und klicken Sie dann auf **AKTIVIEREN**.

## 2.2. Digital Identity Protection konfigurieren

1. Rufen Sie https://central.bitdefender.com auf und melden Sie sich bei Ihrem Benutzerkonto an.
   Wenn Sie noch kein Konto haben, klicken Sie auf **Benutzerkonto erstellen** und geben Sie dann Ihren vollständigen Namen, eine E-Mail-Adresse und ein Passwort ein.
2. Rufen Sie den Bereich Digital Identity Protection auf.
   Die Willkommensseite wird angezeigt.
3. Klicken Sie auf **STARTEN**.
4. Sie werden nun darüber informiert, welche Informationen Sie angeben müssen. Ihre Daten werden grundsätzlich nur verschlüsselt und sicher verwahrt.

Klicken Sie auf **WEITER**.

5. Geben Sie Ihren Vornamen, Ihren zweiten Vornamen (falls vorhanden) und Ihren Nachnamen in die entsprechenden Felder ein, und klicken Sie dann auf **WEITER**.
6. Geben Sie Ihre E-Mail-Adresse ein und klicken Sie auf **WEITER**.
   Stellen Sie sicher, dass es sich dabei um eine gültige E-Mail-Adresse handelt, auf die Sie zugreifen können.
7. An die von Ihnen angegebene Adresse wird ein Sicherheitscode gesendet.
   Öffnen Sie die E-Mail, kopieren Sie den Code und fügen Sie ihn in das entsprechende Feld ein.
   Klicken Sie danach auf **PRÜFEN**.
8. Wählen Sie Ihr Land und geben Sie Ihre Telefonnummer ein und klicken Sie danach auf **WEITER**.
9. Sie sollten kurz darauf einen Sicherheitscode erhalten.
   Geben Sie den Code ein und klicken Sie dann auf **PRÜFEN**.
10. Klicken Sie nach Abschluss der anfänglichen Prüfung auf **ABSCHLIEßEN**.

> **Notiz**
> Sie werden benachrichtigt, wenn bei dieser anfänglichen Überprüfung Datenpannen, persönlich identifizierbare Informationen oder mögliche Versuche von Identitätsbetrug gefunden werden.

Die Einrichtung von Bitdefender Digital Identity Protection ist damit abgeschlossen.

## 2.3. Ihren Digitalen Fußabdruck, Datenpannen und möglichen Identitätsbetrug überprüfen

Nachdem Sie die Einrichtung abgeschlossen haben, führt Bitdefender Digital Identity Protection einen Online-Check durch, um möglichem Identitätsbetrug, Datenpannen und persönlich identifizierbaren Informationen im öffentlich zugänglichem Internet auf die Spur zu kommen. Wir empfehlen, alle Informationen in den Reitern **DIGITALER FUßABDRUCK**, **DATENPANNEN** und **ÜBERPRÜFUNG AUF IDENTITÄTSBETRUG** genau zu prüfen.


- Überprüfen Ihres digitalen Fußabdrucks (Seite 10)
- Überprüfen von Datenpannen (Seite 11)
- Überprüfen von möglichem Identitätsbetrug (Seite 12)


## 2.4. Verbessern Sie die Prüfung

Wir nutzen die von Ihnen bereitgestellten Daten, um das öffentlich zugängliche Internet sowie das Dark Web auf mögliche Aktivitäten zu überwachen, die sich negativ auf Ihre Privatsphäre oder Ihren guten Ruf auswirken könnten.

Wenn Sie eine weitere E-Mail-Adresse oder eine weitere Telefonnummer hinzufügen möchten, klicken Sie auf ⊕, dann auf **E-MAIL-ADRESSE HINZUFÜGEN** oder **TELEFONNUMMER HINZUFÜGEN** und folgen Sie den Anweisungen.

# 3. DASHBOARD

Im Dashboard werden alle Informationen aus den Bereichen **DIGITALER FUßABDRUCK**, **DATENPANNEN** und **ÜBERPRÜFUNG AUF IDENTITÄTSBETRUG** zusammengefasst.

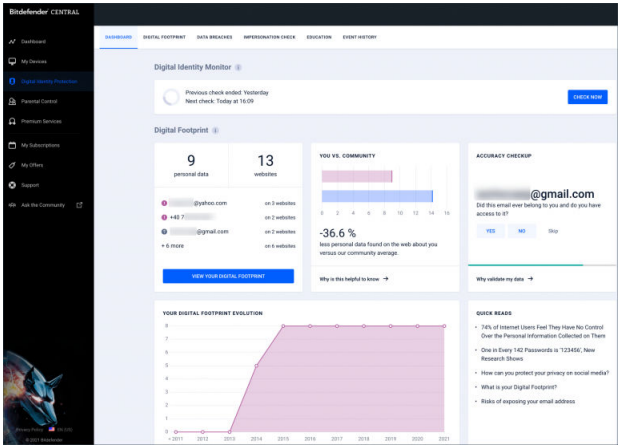
Sie finden dort die folgenden Informationen:

- Ihre offengelegten Daten und Ihre Quellen im Netz
- Die durchschnittliche Anzahl der offengelegten Daten unter allen Nutzern
- Die Entwicklung Ihres digitalen Fußabdrucks
- Datenschutzrelevante Inhalte
- Datenpannen
- Die durchschnittliche Anzahl der Datenpannen unter allen Nutzern

## 3.1. Identitätsüberwachung

Bitdefenders System sucht ausschließlich anhand zutreffender Informationen nach neuen personenbezogenen Daten, die im offenen Internet oder im Darknet veröffentlicht wurden und überprüft alle wichtigen sozialen Netzwerke nach Anzeichen von Identitätsbetrug.

Klicken Sie auf **JETZT PRÜFEN**, um einen Online-Scan durchzuführen.



# 4. DIGITALER FUßABDRUCK

Hier werden Ihre persönlich identifizierbaren Informationen und ihre Quellen angezeigt. Es liegt an Ihnen zu beurteilen, ob die Offenlegung der Informationen im Internet eine Bedrohung darstellt.

Unsere KI-gestützte Überwachung ist zur Erkennung neuer Bedrohungen in hohem Maße auf zutreffende Daten angewiesen. Lassen Sie uns daher bitte wissen, ob die Informationen zutreffen oder nicht.

Sobald Sie bestätigen, dass Daten zu Ihnen gehören, fügen wir sie unserem Überwachungssystem hinzu und verbessern so die Chancen, in Zukunft weitere Informationen zu finden.

## 4.1. Überprüfen Ihres digitalen Fußabdrucks

So überprüfen Sie Ihren digitalen Fußabdruck:

1. Rufen Sie den Reiter **DIGITALER FUßABDRUCK** auf.
2. Informationen, die noch nicht bestätigt wurden, erscheinen mit dem Option **Bestätigen** auf der rechten Seite. Klicken Sie auf **Bestätigen** und danach auf Ja oder Nein.

> **Notiz**
> Jede bestätigte Information wird unserem Überwachungsalgorithmus hinzugefügt, wodurch die Ergebnisgenauigkeit unserer Dienste verbessert wird. Informationen, die verworfen werden, werden nicht mehr angezeigt, bleiben aber weiterhin im Internet verfügbar.

# 5. DATENSCHUTZVERLETZUNGEN

Wenn es Hackern gelingt, die Sicherheitsvorkehrungen eines Unternehmens zu umgehen und an Ihre persönlichen Daten zu gelangen, um sie im Darknet zu verkaufen, spricht man von Datenpannen. In den meisten Fällen haben es Cyberkriminelle auf Anmeldedaten, persönlich identifizierbare Informationen (PII), medizinische Daten und Bankdaten abgesehen.

Jedes Unternehmen oder jeder Dienst kann Opfer von Datenpannen werden, doch mit Größe des Kundenstamms steigt auch die Attraktivität eines Ziels. Datenlecks betreffen in der Regel Namen, E-Mail-Adressen, Benutzernamen, Passwörter, Postanschriften, Telefonnummern, Sozialversicherungsnummern (SSN) und Kreditkartendaten (Nummer, Ablaufdatum, CVV).

## 5.1. Überprüfen von Datenpannen

So können Sie Ihren Datenpannen einsehen:

1. Rufen Sie den Reiter **DATENPANNEN** auf.
2. Unter einigen Einträgen finden Sie eine Liste mit Aktionen, die zur Absicherung Ihres Benutzerkontos erforderlich sind. Klicken Sie nach Abschluss einer Aktion auf das nebenstehende Kästchen, um die Durchführung zu bestätigen.

   Wenn Sie sich nicht sicher sind, wie eine Aufgabe durchzuführen ist, können Sie jederzeit auf den Link in der Aufgabenbeschreibung klicken. Sie werden dann auf eine Seite weitergeleitet, auf der Sie alle erforderlichen Schritte finden.

   Nicht alle Datenpannen können auf so behoben werden. Bei einigen, wie z. B. **Sammlung Nr. 1**, werden keine Schritte angezeigt. Stattdessen werden Sie zu Artikeln im Internet weitergeleitet, in denen Sie weitere Hilfe finden können.

> **Notiz**
> Bitdefender speichert oder verarbeitet keine personenbezogenen Daten. Es werden nur Verweise auf potenzielle Datenschutzverletzungen aufbewahrt, ohne sensible Daten einzubeziehen.

# 6. ÜBERPRÜFUNG AUF IDENTITÄTSBETRUG

Kriminelle, die im Fachjargon als "Pretexter" bezeichnet werden, sind sehr geschickt darin, sich als jemand anders auszugeben. Sie schlüpfen dabei in die Rolle einer vertrauenswürdigen Person, um ihre Opfer zu täuschen und sich Zugang zu sensiblen Informationen zu verschaffen. Die Praxis des "Pretexting" ist definiert als das Vortäuschen der Identität einer anderen Person, um den Empfänger dazu zu bringen, sensible Daten wie Passwörter, Kreditkartennummern oder andere vertrauliche Informationen preiszugeben.

Bitdefender Digital Identity Protection überwacht 25 Social-Media-Plattformen und informiert Sie umgehend über Profile, bei denen der Verdacht auf Identitätsbetrug besteht.

## 6.1. Überprüfen von möglichem Identitätsbetrug

Im Reiter **ÜBERPRÜFUNG AUF IDENTITÄTSBETRUG** werden alle potenziellen Versuche angezeigt. Für jeden Fund stehen drei Möglichkeiten zur Auswahl:

- Es handelt sich um versuchten Identitätsbetrug
- Es handelt sich um Ihr eigenes Profil
- Es handelt sich um ein fremdes Profil

Je nach Auswahl empfiehlt Bitdefender Digital Identity Protection konkrete Schritte, um das Problem zu lösen. Sie können jeden Schritt nach Abschluss als **Erledigt** markieren.

# 7. NEWS

Der Reiter "News" dient als Wissensdatenbank, in der Benutzer weiterführende Informationen zum Schutz ihrer digitalen Identität finden können.

Die Artikel hier können in die folgenden Kategorien eingeteilt werden:

- Schwachstellen
- Sicherheitsrisiken
- Identitätsprüfung

Klicken Sie zum Lesen des vollständigen Artikels auf den entsprechenden **Lesen Sie mehr**-Link.

# 8. EREIGNISVERLAUF

Der Bereich Ereignisverlauf dient der anhaltenden Kommunikation mit unseren Benutzern. Hier finden Sie eine chronologisch geordnete Liste von Ereignissen im Zusammenhang mit dem Schutz Ihrer digitalen Identität.

Neben neu entdeckten Bedrohungen (falls vorhanden) finden Sie auf dieser Seite auch nützliche Tipps zum richtigen Verhalten im Internet, um sich besser gegen mögliche Verletzungen Ihrer Privatsphäre zu wappnen.

Im Ereignisverlauf finden Sie die folgenden Informationen:

- Durchgeführte Aktionen
- Updates des Dienstes
- Datenschutzverletzungen

# 9. HÄUFIG GESTELLTE FRAGEN

**Warum ist es heute so wichtig, die Privatsphäre im Internet zu schützen?**

Online-Privatsphäre bedeutet, Ihre persönlichen und finanziellen Daten vor Cyberkriminellen zu schützen. Für persönlich identifizierbare Informationen lassen sich im Internet hohe Preise erzielen. Wenn Sie von Datenlecks betroffen sind, kann dies schnell finanzielle Verluste nach sich ziehen. Sie benötigen einen zuverlässigen Dienst, der Ihre Identität kontinuierlich überwacht und schützt. Nur so können Sie sicherstellen, dass Ihre privaten Daten auch privat bleiben.

**Was ist ein digitaler Fußabdruck?**

Ihr digitaler Fußabdruck sind Ihre gesammelten Online-Aktivitäten. Jede Anmeldung bei Ihren Social-Media-Konten, jede Banktransaktion, jeder Online-Einkauf kann von Datenschutzverletzungen betroffen sein. Sie müssen sich jederzeit darüber bewusst sein, wie Ihre persönlichen und finanziellen Daten gespeichert werden und wie der Umgang damit aussieht - und die notwendigen Schritte unternehmen, um sie zu schützen.

**Was sind Datenschutzverletzungen und wie wirken sie sich auf meine Benutzerkonten aus?**

Datenschutzverletzungen sind Sicherheitsvorfälle, bei denen private Daten in ungeschützte Umgebungen gelangen. Diese können dann von Cyberkriminellen auf der ganzen Welt ausgenutzt werden, um sich Zugang zu Ihrer Online-Identität zu verschaffen. Datenschutzverletzungen können Auswirkungen auf Ihre Kreditwürdigkeit, Ihre Krankenversicherung, Ihre Rentenversicherung und vieles mehr haben.

**Wie hilft mir Bitdefender Digital Identity Protection, meine Online-Privatsphäre zu schützen?**

Bitdefender Digital Identity Protection überwacht fortlaufend Ihre persönlichen Daten und warnt Sie im Falle von Datenverletzungen in Echtzeit. So können Sie Ihre Passwörter ändern und Ihre Konten sichern, um finanzielle Schäden oder den Missbrauch Ihrer Social-Media-Profile zu verhindern.

**Wo sucht Bitdefender Digital Identity Protection nach meinen Daten?**

Bitdefender Digital Identity Protection durchsucht nicht nur die öffentlichen Bereiche des Internets (soziale Netzwerke, Posts, Blogs, Foren, Datenhändler, Publikationen, Offline-Datenbanken), sondern auch die Marktplätze des Dark Web, wo Cyberkriminelle mit Informationen handeln, die aus Datenverletzungen stammen.

**Wie unterscheidet sich Bitdefender Digital Identity Protection von anderen (kostenlosen) Diensten?**

Bitdefender Digital Identity Protection verfügt wie kein anderer Dienst über Möglichkeiten zur Überwachung großer Mengen auch qualitativ hochwertiger Daten im Dark Web. Die Informationen aus dem Dark Web werden von uns aufbereitet und de-dupliziert, um Fehlalarme zu reduzieren.

**Wie kann ich den Dienst nutzen? Ist ein Download erforderlich?**

Bitdefender Digital Identity Protection ist ein Online-Dienst, es ist also kein Download erforderlich. Sie erhalten Zugriff auf ein Online-Dashboard, über das Sie alle Ihre Benutzerkonten in Echtzeit überwachen können.

**Wie werde ich über zukünftige Datenlecks informiert?**

Um über zukünftige Datenlecks informiert zu werden, müssen Sie sich lediglich über Ihr Online-Dashboard für die E-Mail-Benachrichtigungen anmelden. Im Anschluss erhalten Sie von der Bitdefender Digital Identity Protection Warnungen bei Privatsphäreverletzungen und Sicherheitsberichte.

# 10. HILFE UND SUPPORT

## 10.1. Hier wird Ihnen geholfen

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

## 10.2. 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.

### 10.2.1. Bitdefender-Support-Center

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

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

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

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

### 10.2.2. 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

### 10.2.3. Bitdefender Cyberpedia

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

Die Bitdefender Cyberpedia finden Sie hier:

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

## 10.3. 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/

### 10.3.1. Lokale Vertriebspartner

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

So finden Sie einen Bitdefender Distributor in Ihrem Land:

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

# GLOSSAR

**Aktivierungscode**

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

**ActiveX**

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

**Advanced Persistent Threat**

Advanced Persistent Threat (APT) nutzen Sicherheitslücken im System, um wichtige Daten zu stehlen und an ihre Quellen zu übermitteln. Organisationen, Unternehmen und Regierungsbehörden sind eine große Zielgruppe, die von dieser Bedrohung ins Visier genommen wird. Advanced Persistent Threats sollen so lange wie möglich unentdeckt bleiben. Während dieser Zeit sollen sie das System überwachen und wichtige Daten sammeln, ohne dabei die Zielcomputer zu beschädigen. Die Bedrohung wird durch PDF-Dateien oder Office-Dokumente in das Netzwerk eingebracht, die keinen Verdacht erregen, so dass jeder Benutzer diese Dateien ausführen kann.

**Adware**

Adware wird häufig mit einer anderen Anwendung kombiniert, die kostenlos ist, solange der Nutzer die Adware akzeptiert. Adware-

Anwendungen werden in der Regel installiert, nachdem der Nutzer einer Lizenzvereinbarung zugestimmt hat. In der Lizenzvereinbarung wird auch der Zweck der Anwendung genannt, und somit liegt keine Rechtswidrigkeit vor. Allerdings können Popup-Anzeigen mit der Zeit sehr lästig werden und in manchen Fällen die Systemperformance beeinträchtigen. Zudem kann aufgrund der Daten, die manche dieser Programme sammeln, die Privatsphäre von Nutzern verletzt werden, die sich über die Bedingungen in der Lizenzvereinbarung nicht völlig im Klaren waren.

**Archiv**

Ein Datenträger, ein Magnetband oder ein Ordner mit Dateien, die von einem Backup erzeugt wurden.

Eine Datei, die eine oder mehrere Dateien in einem komprimierten Format enthält.

**Hintertür**

Eine Sicherheitslücke eines Systems, die der Entwickler oder Verwalter absichtlich hinterlässt.Der Grund dafür muss nicht immer bösartig sein.Manche Betriebssysteme haben schon bei der Fabrikation privilegierte Konten, damit diese von den Kundendienst-Technikern oder Programmierern der Hersteller benutzt werden können.

**Bootsektor**

Der erste Sektor einer Festplatte oder Diskette.Hier liegen Daten, die das Betriebssystem zum Booten (Starten) braucht.

**Bootvirus**

Eine Bedrohung, der den Bootsektor einer Festplatte oder eines Diskettenlaufwerks infiziert. Beim Versuch von einer Diskette, die mit einem Bootvirus infiziert ist, zu booten wird diese Bedrohung im Arbeitsspeicher aktiviert. Bei jedem Neustart wird die Bedrohung so im Arbeitsspeicher aktiviert und überträgt sich auf eingelegte Wechselmedien.

**Botnet**

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

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

**Browser**

Kurzform für Web-Browser, ein Programm, mit dem Internetseiten aufgerufen und angezeigt werden können. Bekannte Browser sind Microsoft Internet Explorer, Mozilla Firefox und Google Chrome. Dies sind graphische Browser, was bedeutet, dass sie sowohl Grafiken als auch Texte anzeigen können. Weiterhin können die meisten Browser Multimedia-Daten wie Klang- und Videodateien anzeigen, wobei sie für diverse Formate Plug-Ins (zusätzliche Softwarekomponenten) benutzen.

**Brute-Force-Angriff**

Ein Angriff mit dem Ziel, sich Zugang zu einem passwortgeschützten System zu verschaffen, bei dem in schneller Abfolge häufige Passwortkombinationen durchprobiert werden.

**Befehlszeile**

Die Befehlszeile ist eine zeichenorientierte Benutzerschnittstelle. Die Kommunikation zwischen Benutzer und Computer findet ausschließlich durch die Eingabe von bestimmten Befehlen statt, die sich aus einzelnen Buchstabenfolgen zusammensetzen. Als Eingabegerät wird eine Tastatur benutzt. Die Verwendung einer Maus ist nicht möglich. Auf der Befehlszeile werden die einzelnen Anweisungen in einer bestimmten Befehlssprache eingegeben, die vom Computer und seiner Software ausgewertet und mit den entsprechenden Ergebnissen auf dem Ausgabegerät (meistens ein Monitor) wieder an den Benutzer übergeben werden.

**Cookies**

In der Internetbranche werden mit Cookies kleine Dateien bezeichnet, die Daten über einzelne Computer enthalten und die von den Werbetreibenden analysiert und verwendet werden, um die Interessen und Vorlieben der Benutzer herauszufinden. Die Cookie-Technologie wird stetig weiterentwickelt mit dem Ziel Benutzern nur noch solche Werbung anzuzeigen, die ihren Interessen entspricht. Für viele ist dies ein zweischneidiges Schwert. Einerseits ist es praktisch, nur Anzeigen zu sehen, an denen man interessiert ist. Anderseits bedeutet es, dass Online-Aktivitäten der Benutzer gewissermaßen auf Schritt und "Klick"

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

**Cybermobbing**

Wenn Altersgenossen oder Fremde absichtlich Kinder misshandeln, um sie körperlich zu verletzen. Um emotionale Schäden anzurichten, schicken die Täter verletzende Nachrichten oder unvorteilhafte Fotos, so dass sich ihre Opfer von anderen isolieren oder entmutigt werden.

**Wörterbuchangriff**

Ein Angriff mit dem Ziel, sich Zugang zu einem passwortgeschützten System zu verschaffen, bei dem alle möglichen Wörter aus einem Wörterbuch als potenzielle Passwörter eingegeben werden. Dieselbe Methode wird auch verwendet um Schlüssel für verschlüsselte Nachrichten oder Dokumente zu erraten. Wörterbuchangriffe funktionieren, weil viele Benutzer kurze, leicht zu erratende Wörter als Passwörter benutzen.

**Laufwerk**

Ein Gerät, das rotierende Speichermedien lesen und beschreiben kann. Ein Festplatten-Laufwerk liest und beschreibt Festplatten. Ein Disketten-Laufwerk liest und beschreibt Disketten. Laufwerke können sowohl interner (im Rechner eingebaut) als auch externer (in einem Gehäuse, das an den Rechner angeschlossen wird) Art sein.

**Download**

Kopiert Daten (gewöhnlich eine ganze Datei) von einer Hauptquelle auf ein Peripheriegerät.Der Begriff bezeichnet oft den Kopiervorgang von einem Online Service auf den eigenen Rechner.Download oder Herunterladen kann auch das Kopieren einer Datei von einem Netzwerkserver auf einen Netzwerkrechner bedeuten.

**E-Mail**

Elektronische Post. Ein Dienst, der Nachrichten an andere Rechner über ein lokales oder ein globales Netzwerk übermittelt.

**Ereignisse**

Ereignisse oder Erscheinungen, die in einem Programm vorkommen.Ereignisse können Benutzeraktionen, wie zum Beispiel

Mausklicks oder Tastatureingaben, oder Systemereignisse, wie zum Beispiel ungenügender Speicher, sein.

**Exploits**

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

**Fehlalarme**

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

**Dateinamenerweiterung**

Der Teil hinter dem Punkt im Dateinamen. Die Erweiterung oder Extension beschreibt die Art der Daten, die in einer Datei gespeichert sind. Viele Betriebssysteme benutzen Dateierweiterungen, z.B. Unix, VMS, MS-DOS. Sie sind gewöhnlich ein bis drei Buchstaben lange (alte Betriebssysteme können oft nicht mehr als drei Buchstaben unterstützen). Beispiele sind "exe" ausführbare Dateien, "ps" für PostScript oder "txt" für Text-Dateien.

**Heuristik**

Eine Methode, um neue Bedrohungen zu identifizieren. Diese Scan-Methode benötigt keine konkreten Bedrohungsinformationen. Der Vorteil eines heuristischen Scans ist, dass man nicht von einer neuen Variante einer alten Bedrohung getäuscht werden kann. Manchmal kann jedoch auch ein verdächtiger Code in einem normalen Programm gemeldet werden, ein sogenannter Fehlalarm oder "falsch-positive Meldung" wird angezeigt.

**Honeypot**

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

**IP**

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

**Java-Applet**

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

Obwohl Applets auf dem Client laufen, können diese keine Daten auf der Clientmaschine lesen oder schreiben. Zusätzlich sind die Applets weiter begrenzt, so dass sie nur Daten aus der Domäne lesen und beschreiben können, die sie unterstützen.

**Keylogger**

Ein Keylogger ist eine Anwendung, die alle Ihre Tastenanschläge aufzeichnet. Keylogger sind an sich nicht schädlich. Sie können auch legitim eingesetzt werden, um beispielsweise die Aktivitäten von Angestellten oder Kindern zu überwachen. Sie werden jedoch zunehmend von Cyber-Kriminellen mit bösartiger Absicht eingesetzt (um beispielsweise private Daten wie Benutzernamen oder Passwörter zu sammeln).

**Makrovirus**

Eine Bedrohungsart, die in einem Dokument als eingebettetes Makro verschlüsselt wird. Viele Anwendungen, wie Microsoft Word und Excel, unterstützen leistungsstarke Makrosprachen. Diese Anwendungen ermöglichen das Einbetten eines Makros in ein Dokument, welches dann bei jedem Öffnen des Dokuments ausgeführt wird.Ein Makro ist eine Aufzeichnung des Ablaufs von Routineaufgaben innerhalb des makrofähigen Programms, das dann immer wieder verwendet werden kann.

**Mail-Client**

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

**Arbeitsspeicher**

Interne Speicherzonen im Rechner.Der Begriff Arbeitsspeicher bedeutet Datenträger in Form von sehr schnellen Chips.Das Wort Speicher ist der Speicherplatz, der sich auf Magnetbändern oder Datenträgern befindet.Jeder Rechner hat eine gewisse Menge Arbeitsspeicher.Dieser wird auch Hauptspeicher oder RAM genannt.

**Nicht-heuristisch**

Diese Scan-Methode benötigt konkrete Bedrohungsinformationen. Der Vorteil eines nicht-heuristischen Scans ist, dass er nicht von einer Scheinbedrohung getäuscht werden kann und so Fehlalarme verhindert.

**Online-Missbrauch**

Wenn Personen versuchen, Minderjährige oder Jugendliche anzusprechen, um sie in illegale sexuelle Aktivitäten zu verwickeln. Soziale Netzwerke sind der ideale Ort, um verletzlichen Kindern nachzustellen und sie zu sexuellen Aktivitäten zu verführen, sei es online oder persönlich.

**Komprimierte Programme**

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

Ein Programm zum Komprimieren von Dateien würde jedoch die Leerzeichen durch ein spezielles Zeichen der Leerzeichenreihe, gefolgt von der Anzahl der zu ersetzenden Leerzeichen, ersetzen. In diesem Fall würden für die zehn Leerzeichen nur zwei Bytes benötigt. Dies ist nur eine Komprimierungstechnik - es gibt noch viele weitere.

**Pfad**

Zeigt die Stelle an, an der sich eine Datei auf einem Computer befindet. Diese Pfadangaben enthalten gewöhnlich den hierarchischen Aufbau des Dateiverzeichnisses von oben nach unten.

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

**Phishing**

Das Senden einer E-Mail an einen Benutzer, in der der Sender sich als Vertreter eines legitimen Unternehmens ausgibt und versucht, den Empfänger so zu manipulieren, dass er persönliche Informationen preisgibt, die dann zum Diebstahl der Identität verwendet werden können. Die E-Mail leitet den Benutzer dann auf eine Webseite, auf der er aufgefordert wird, vertrauliche Daten wie Kreditkartennummern, TANs

oder PINs preiszugeben. Es wird oft vorgegeben, dass dies aus Gründen der Aktualisierung geschehen soll. Diese Webseiten sind jedoch gefälscht und wurden eigens für den Diebstahl dieser Daten eingerichtet.

**Photon**

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

**Polymorphic virus**

Eine Bedrohung, die ihre Form mit jeder Datei, die sie infiziert, ändert. Da diese Bedrohungen kein beständiges binäres Muster haben, sind sie sehr schwer zu erkennen.

**Port**

Eine Schnittstelle an einem Computer, an die ein Gerät angeschlossen werden kann. PCs haben verschiedene Arten von Anschlüssen. Intern gibt es mehrere Anschlüsse für den Anschluss von Laufwerken, Bildschirmen und Tastaturen. Extern haben PCs Anschlüsse für den Anschluss von Modems, Druckern, Mäusen und anderen Peripheriegeräten.

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

**Ransomware**

Ransomware ist bösartige Software, die das System des Opfers sperrt und nur gegen ein Lösegeld wieder entfernt wird. CryptoLocker, CryptoWall und TeslaWall sind einige bekanntere Beispiele für Ransomware.

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

**Berichtsdatei**

Eine Datei, die stattgefundene Aktivitäten aufzeichnet.Zum Beispiel speichert BitDefender eine Logdatei mit die geprüften Pfaden, Ordnern und der Archivanzahl, aber auch die geprüften, infizierten oder verdächtigen Dateien.

**Rootkit**

Ein Rootkit ist eine Sammlung von Software-Tools, die den Zugriff auf ein System auf Administratorebene ermöglichen. Der Begriff wurde erstmals für UNIX-Betriebssysteme verwendet und bezog sich auf neu kompilierte Tools, die Eindringlingen administrative Rechte verschafften und es ihnen ermöglichten, ihre Anwesenheit zu verbergen, um der Erkennung durch den Systemadministrator zu entgehen.

Die Hauptaufgabe von Rootkits besteht darin, Prozesse, Dateien, Logins und Protokolle zu verbergen. Sie können auch Daten von Terminals, Netzwerkverbindungen oder Peripheriegeräten abfangen, wenn sie die entsprechende Software enthalten.

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

**Skript**

Ein anderer Begriff für Makro- oder Batchdatei. Ein Skript ist eine Befehlsliste, die ohne Benutzereingriff ausgeführt werden kann.

**Spam**

Junk-E-Mail oder Junk-Beiträge in Newsgroups. Im Allgemeinen versteht man darunter jede Art von unerwünschter E-Mail.

**Spyware**

Software, die unentdeckt vom Nutzer private und geheime Anwenderdaten über seine Internetverbindung abgreift. Dies geschieht in der Regel zu Werbezwecken. Typischerweise sind Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Shareware-Programmen enthalten, die aus dem Internet heruntergeladen werden können. Die große Mehrzahl von Shareware- und Freeware-Anwendungen ist natürlich frei von Spyware. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an einen Dritten. Spyware kann auch Informationen über E-Mail-Adressen und sogar Passwörter und Kreditkartennummern sammeln.

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

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

**Systemstartelemente**

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

**Abonnement**

Ein Kaufvertrag, der Benutzern das Recht einräumt, ein bestimmtes Produkt oder eine Dienstleistung auf einer bestimmten Anzahl von Geräten und für einen bestimmten Zeitraum in Anspruch zu nehmen. Ein abgelaufenes Abonnement kann unter Verwendung der vom Nutzer beim Ersterwerb angegebenen Informationen automatisch verlängert werden.

**Taskleiste**

Die Symbolleiste wurde mit Windows 95 eingeführt und befindet sich auf der Windows Taskleiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet). Sie enthält kleine Icons zur Information und zum leichteren Zugriff, zum Beispiel: Fax, Drucker, Modem, Lautstärke und mehr. Um auf die Details und Steuerungen zuzugreifen, ist ein Doppelklick oder ein Klick mit der rechten Maustaste erforderlich.

**TCP/IP**

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

**Bedrohung**

Ein Programm oder ein Stück Code, das auf einen Rechner kopiert wird und sich allein ausführt, ohne dass es der Besitzer des Rechners will oder merkt. Die meisten Bedrohungen können sich auch selbst vervielfältigen. Alle Computerbedrohungen wurden von Menschen programmiert. Eine einfache Bedrohung, die sich immer wieder vervielfältigen kann, ist sehr einfach zu programmieren. Sogar eine solch einfache Bedrohung kann gefährlich sein, da sie im Handumdrehen sämtlichen Arbeitsspeicher belegen und so das System lahmlegen kann. Noch gefährlicher sind Bedrohungen, die sich über Netzwerke hinweg selbst weiterversenden und Sicherheitssysteme umgehen.

**Update der Bedrohungsinformationen**

Das binäre Muster einer Bedrohung, wird von der Sicherheitslösung zur Erkennung und Beseitigung einer Bedrohung genutzt.

**Trojaner**

Ein bösartiges Programm, das sich als eine legitime Anwendung ausgibt. Anders als Schad-Software und Würmer vervielfältigen sich Trojaner nicht selbst, können aber dennoch großen Schaden anrichten. Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Bedrohungen zu befreien, stattdessen aber den Rechner infiziert.

Der Begriff entstammt einer Geschichte in Homer's "Ilias", in der die Griechen Ihren Feinden, den Trojanern, angeblich als Sühnegabe ein hölzernes Pferd schenkten.Aber, nachdem die Trojaner das Pferd innerhalb der Stadtmauern gebracht hatten, kamen die in dem Bauch des hölzernen Pferdes versteckten Soldaten heraus, öffneten die Tore der Stadt und ermöglichten somit ihren Landsmännern in die Stadt einzudringen und auf diese Weise Troja zu besetzen.

**Update**

Neue Softwareversionen oder Hardwareprodukte, die eine ältere Version ersetzen.Die Update-Installationsroutine sucht nach älteren Versionen auf dem Rechner, da sonst kein Update installiert werden kann.

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

**Virtual Private Network (VPN)**

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

**Wurm**

Ein Programm, das sich selbst über ein Netzwerk ausbreitet und sich dabei selbst reproduziert. Es kann sich nicht an andere Programme anhängen.