BENUTZERHANDBUCH

Bitdefender CONSUMER SOLUTIONS

Mobile Security for iOS

Bitdefender Mobile Security for iOS

Bedienungsanleitung

Veröffentlichungsdatum: 02.10.2023

Impressum

Bitdefender

Inhaltsverzeichnis

Über diese Anleitung 1
Zielsetzung und Zielgruppe 1
Über dieses Handbuch 1
Konventionen in diesem Handbuch 1
Typografie 1
Zusätzliche Hinweise 2
Ihre Mithilfe 2
1. Was ist Bitdefender Mobile Security for iOS? 4
2. Erste Schritte 5
2.1. Systemanforderungen 5
2.2. Installation von Bitdefender Mobile Security for iOS 5
2.3. Melden Sie sich bei Ihrem Bitdefender-Konto an 6
2.4. Dashboard 7
3. Funktionen und Merkmale 10
3.1. Scan 10
3.2. Betrugsalarm 10
3.2.1. So richten Sie den Betrugsalarm ein 11
3.3. Internet-Schutz 12
3.3.1. Bitdefender-Benachrichtigung 13
3.4. VPN 14
3.4.1. Abonnements 16
3.5. Kontoschutz 17
4. Über Bitdefender Central 19
4.1. Aufrufen von Bitdefender Central 19
4.2. Zwei-Faktor-Authentifzierung 20
4.2.1. Aktivieren der Zwei-Faktor-Authentifizierung 20
4.3. Hinzufügen vertrauenswürdiger Geräte 22
4.4. Meine Geräte 22
4.4.1. Hinzufügen eines neuen Geräts 23
4.4.2. Persönliche Anpassungen 24
4.4.3. Fernzugriffsaktionen 24
4.5. Aktivität 26
4.6. Meine Abonnements 26
4.6.1. Verfügbare Abonnements anzeigen 26
4.6.2. Abonnement aktivieren 27
4.6.3. Abonnement verlängern 27
4.7. Benachrichtigungen 29
5. Häufig gestellte Fragen 30
6. Hilfe und Support 31

6.1. Hier wird Ihnen geholfen 31
6.2. Online-Ressourcen 31
6.2.1. Bitdefender-Support-Center 31
6.2.2. Die Bitdefender Experten Community 32
6.2.3. Bitdefender Cyberpedia 32
6.3. Kontaktinformation 33
6.3.1. Lokale Vertriebspartner 33
Glossar 34

ÜBER DIESE ANLEITUNG

Zielsetzung und Zielgruppe

Dieses Handbuch richtet sich an alle iOS-Benutzer, die sich für den Einsatz von Bitdefender Mobile Security for iOS als Sicherheitslösung für ihre Mobilgeräte entschieden haben. Die enthaltenen Informationen setzen keine besonderen technischen Kenntnisse voraus, sondern dienen allen im Umgang mit Apple-Geräten erfahrenen Benutzern als leicht verständliche Anleitung.

Lesen Sie, wie Sie Bitdefender Mobile Security for iOS konfigurieren und einsetzen, um sich vor Bedrohungen und Malware zu schützen. Wir zeigen Ihnen, wie Sie alles aus Bitdefender herausholen.

Viel Spaß mit diesen nützlichen und informativen Handbuch.

Über dieses Handbuch

Dieses Handbuch behandelt die folgenden Themengebiete:

Erste Schritte (Seite 5)

Starten mit Bitdefender Mobile Security for iOS und der Benutzeroberfläche.

Funktionen und Merkmale (Seite 10)

Erfahren Sie, wie Sie sich mit Bitdefender Mobile Security for iOS vor Bedrohungen und Malware schützen können, indem Sie sich mit den Funktionen und Merkmalen des Programms vertraut machen.

Hilfe und Support (Seite 31)

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 MOBILE SECURITY FOR IOS?

Über das Internet kann man schnell und bequem Rechnungen bezahlen, Urlaube buchen sowie Waren und Dienstleistungen erwerben. Die verstärkte Nutzung dieser Online-Dienste geht jedoch auch mit hohen Risiken einher. Ohne die entsprechenden Sicherheitsvorkehrungen können personenbezogene Daten schnell in die falschen Hände gelangen. Was ist also wichtiger, als der Schutz der Daten, die in unseren Online-Konten und Smartphones zu finden sind?

Mit Bitdefender Mobile Security for iOS können Sie:

- Profitieren Sie von maximalem Schutz bei minimalen Auswirkungen auf die Akkulaufzeit
- Schützen Sie Ihre Daten: Passwörter, Adressen, persönliche und finanzielle Informationen
- Überprüfen Sie Ihr Telefon jederzeit auf Sicherheitslücken und beheben Sie gefährliche Fehlkonfigurationen
- Vermeiden Sie die unbeabsichtigte Preisgabe von Daten und Missbrauch durch installierte Anwendungen
- Scannt Ihr Gerät, um die optimalen Sicherheits- und Privatsphäreeinstellungen für Sie zu ermitteln
- Erhalten Sie Einblicke in Ihre Online-Aktivitäten und einen Überblick über verhinderte Vorfälle
- Überprüfen Sie Ihre Benutzerkonten auf Datenpannen und Datenlecks
- Verschlüsseln Sie Ihren Internetdatenverkehr mit dem integrierten VPN

Bitdefender Mobile Security for iOS wird kostenlos zur Verfügung gestellt und muss mit einem Bitdefender-Konto aktiviert werden. Einige wichtige Funktionen von Bitdefender, so z. B. unser 'Internet-Schutz', erfordern jedoch ein kostenpflichtiges Abonnement, um für unsere Nutzer zugänglich zu sein.

2. ERSTE SCHRITTE

2.1. Systemanforderungen

Bitdefender Mobile Security for iOS läuft auf jedem Gerät ab iOS 12 und benötigt eine aktive Internetverbindung, um aktiviert zu werden und um zu erkennen, ob Ihre Online-Konten von Datenlecks betroffen sind.

2.2. Installation von Bitdefender Mobile Security for iOS

- **Über Bitdefender Central**
  - Für iOS
    1. Rufen Sie{1}Bitdefender Central{2} auf.
    2. Rufen Sie den Bereich {1}Meine Geräte{2} auf.
    3. Tippen Sie auf **SCHUTZ INSTALLIEREN** und dann auf **Dieses Gerät schützen**.
    4. Wählen Sie den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, tippen Sie auf die entsprechende Schaltfläche.
    5. Sie werden zur **App Store**-App weitergeleitet. Tippen Sie im App Store auf Installieren.
  - Für Windows, macOS, Android
    1. Zugang Bitdefender-Zentrale.
    2. Wähle aus **Meine Geräte** Tafel.
    3. Tippen Sie auf **SCHUTZ INSTALLIEREN** und dann auf **Andere Geräte schützen**.
    4. Wählen Sie den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, drücken Sie auf die entsprechende Schaltfläche.
    5. Tippen Sie auf **DOWNLOAD LINK SENDEN**.
    6. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und tippen Sie auf **E-MAIL VERSENDEN**. Bitte beachten

Sie, dass der generierte Download-Link nur für die nächsten 24 Stunden gültig ist. Nach Ablauf des Links müssen Sie einen neuen Link generieren. Führen Sie dazu die bereits beschriebenen Schritte erneut aus.

7. Rufen Sie auf dem Gerät, auf dem Bitdefender installiert werden soll, das angegebene E-Mail-Konto auf und tippen Sie in der E-Mail auf die Download-Schaltfläche.

- **Über App Store**
  Suchen Sie nach Bitdefender Mobile Security for iOS, um die App aufzurufen und zu installieren.

Beim ersten Öffnen der App wird ein Einführungsfenster mit Informationen zu den Produktfunktionen angezeigt. Tippen Sie auf Erste Schritte, um das nächste Fenster zu öffnen.

Bevor Sie die Bestätigungsschritte abschließen können, müssen Sie zunächst der Abonnementvereinbarung zustimmen. Bitte nehmen Sie sich einen Moment Zeit, um die Abonnementvereinbarung zu lesen, da Sie hier die Bedingungen finden, unter denen Sie Bitdefender Mobile Security for iOS nutzen dürfen.

Tippen Sie auf **Fortfahren**, um zum nächsten Fenster zu gelangen.

2.3. Melden Sie sich bei Ihrem Bitdefender-Konto an

Zur Verwendung von Bitdefender Mobile Security for iOS müssen Sie Ihr Gerät mit einem Bitdefender-, Facebook-, Google-, Apple-, Microsoft-Konto verknüpfen, indem Sie sich über die App bei Ihrem Konto anmelden. Beim ersten Öffnen der App werden Sie zur Anmeldung bei einem Benutzerkonto aufgefordert.

So verknüpfen Sie Ihr Gerät mit einem Bitdefender-Konto:

1. Geben Sie die E-Mail-Adresse für Ihr Bitdefender-Benutzerkonto in das entsprechende Feld ein, und tippen Sie dann auf **WEITER**. Wenn Sie noch kein Bitdefender-Benutzerkonto haben und eines erstellen möchten, tippen Sie auf den entsprechenden Link und folgen Sie dann den Anweisungen auf dem Bildschirm, bis das Benutzerkonto aktiviert ist.
   Tippen Sie zur Anmeldung mit einem Facebook-, Google-, Apple- oder Microsoft-Konto im Bereich **Oder melded Sie sich an über**

auf den entsprechenden Dienst. Sie werden zur Anmeldeseite des ausgewählten Dienstes weitergeleitet. Befolgen Sie die Anweisungen zur Verknüpfung Ihres Benutzerkontos mit Bitdefender Mobile Security for iOS.

> **Notiz**
> Bitdefender hat keinen Zugriff auf Ihre vertraulichen Informationen, so zum Beispiel das Passwort, das Sie zur Anmeldung in Ihrem Konto verwenden, oder die persönlichen Informationen Ihrer Freunde und Kontakte.

2. Geben Sie Ihr Passwort ein und tippen danach Sie auf **ANMELDEN**.

Von hier aus gelangen Sie auch zur Bitdefender-Datenschutzerklärung.

2.4. Dashboard

Tippen Sie im App-Depot Ihres Geräts auf das Symbol für Bitdefender Mobile Security for iOS, um die Andwendungsoberfläche anzuzeigen.

Beim ersten Aufrufen der App werden Sie aufgefordert, Ihre Zustimmung zur Übermittlung von Bitdefender-Benachrichtigungen zu erteilen. Tippen Sie auf **Zulassen**, um von Bitdefender über alle relevanten Neuigkeiten zu Ihrer App auf dem Laufenden gehalten zu werden. Sie können die Bitdefender-Benachrichtigungen jederzeit unter Einstellungen > Benachrichtigungen > Mobile Security verwalten.

Tippen Sie auf das entsprechende Symbol am unteren Rand des Bildschirms, um den gewünschten Bereich aufzurufen.

Internet-Schutz

Stellen Sie eine sichere Internetnutzung sicher und verhindern Sie, dass weniger sichere Apps auf nicht vertrauenswürdige Domains zugreifen. Weitere Informationen finden Sie unter Internet-Schutz (Seite 12).

VPN

Schützen Sie Ihre Privatsphäre unabhängig davon, welches Netzwerk Sie gerade nutzen, indem Sie Ihre Kommunikation stets verschlüsseln. Weitere Informationen finden Sie unter VPN (Seite 14).

Kontoschutz

Erfahren Sie, ob Ihre E-Mail-Konten von Datenschutzverletzungen betroffen sind. Weitere Informationen finden Sie unter Kontoschutz (Seite 17).

Tippen Sie auf das ···-Symbol Ihres Gerätes, während Sie sich im Hauptmenü der Anwendung befinden, um weitere Optionen anzuzeigen. Die folgenden Optionen werden angezeigt:

- **Käufe wiederherstellen** - Hier können Sie frühere Abonnements, die Sie über Ihr iTunes-Konto erworben haben, wiederherstellen.
- **Einstellungen** - von hier aus haben Sie Zugriff auf:
  - **VPN-Einstellungen**
    - **Vereinbarung** - hier können Sie die Nutzungsbedingungen einsehen, unter denen Sie den Bitdefender VPN-Dienst nutzen dürfen. Wenn Sie auf **Ich bin nicht mehr einverstanden** tippen, können Sie Bitdefender VPN zumindest solange nicht nutzen, bis Sie wieder auf **Ich bin einverstanden** tippen.
    - **Warnung bei offenen WLAN-Netzwerken** - hier können Sie die Produktbenachrichtigung aktivieren oder deaktivieren, die bei jeder Verbindung mit einem ungesicherten WLAN-Netzwerk erscheint.
      Der Zweck dieser Benachrichtigung ist es, Ihnen dabei zu helfen, Ihre Daten durch die Verwendung von Bitdefender VPN vor unbefugten Zugriff zu schützen.
  - **Web-Schutz-Einstellungen**
    - **Vereinbarung** - hier können Sie die Nutzungsbedingungen einsehen, unter denen Sie den Bitdefender-Internet-Schutz-Dienst nutzen dürfen. Wenn Sie auf **Ich bin nicht mehr einverstanden** tippen, können Sie Bitdefender VPN zumindest solange nicht nutzen, bis Sie wieder auf **Ich bin einverstanden** tippen.
    - **Internet-Schutz-Benachrichtigung aktivieren** - Benachrichtigt Sie, dass der Internet-Schutz nach Beendigung einer VPN-Sitzung aktiviert werden kann.
  - **Produktberichte**

- **Feedback** - Hiermit starten Sie Ihre Standard-E-Mail-Anwendung, über die Sie uns Ihre Meinung zur App zukommen lassen können.
- **App-Info** - Hiermit rufen Sie Informationen zur installierten Version sowie die Abonnementvereinbarung, Datenschutzrichtlinie und Informationen zur Einhaltung der Bedingungen von Open-Source-Lizenzen ein.

3. FUNKTIONEN UND MERKMALE

3.1. Scan

Mit Bitdefender Mobile Security for iOS können Sie Ihr Gerät auf Sicherheitslücken und potenzielle Bedrohungen scannen. Ein solcher Scan sucht nach:

- **Betriebssystemversion1}:** Sucht nach den neuesten Updates für Ihre iOS-Version.
- **Passcode/Biometrie:** Prüft, wie gut der Zugriff auf Ihr Gerät gesichert ist.
- **Internet-Schutz:** Überprüft den Status des Internet-Schutzmoduls.
- **Kontoschutz:** Sucht nach überwachten Benutzerkonten, die im Kontoschutzmodul aufgeführt sind.
- **WLAN prüfen:** Überprüft, wie sicher das Netzwerk ist, mit dem Sie gerade verbunden sind.

Der Schutzstatus wird nach einem manuellen Scan ermittelt.

Nach dem ersten Scan werden Sie von Bitdefenders Autopilot-Empfehlungen begrüßt. Der Autopilot ist Ihr persönlicher Sicherheitsberater, der Ihnen kontextbezogene Empfehlungen auf Grundlage Ihrer Gerätenutzung und Anforderungen gibt. Auf diese Weise können Sie wirklich alle Vorteile Ihrer App nutzen.

> **Notiz**
> Beim ersten Aufrufen der App werden Sie aufgefordert, einen Scan durchzuführen.

3.2. Betrugsalarm

Die in Bitdefender Mobile Security für iOS verfügbare Scam Alert-Funktion schützt Apple-Benutzer proaktiv vor Phishing-Betrügereien. Scam Alert für iOS umfasst zwei Schutzebenen, die Betrugsversuche überwachen, die über SMS/MMS-Nachrichten und Kalendereinladungen übermittelt werden:

- **Textnachrichtenfilter (SMS, MMS)**

Diese Funktion identifiziert und filtert unerwünschte SMS- und MMS-Nachrichten.

Eine bösartige SMS/MMS (Short Message Service/Multimedia Messaging Service) bezieht sich auf eine Art von Nachricht, die mit schädlicher Absicht an mobile Geräte gesendet wird. Diese Nachrichten sollen Schwachstellen ausnutzen, Empfänger täuschen oder dem Gerät, den persönlichen Daten oder der Sicherheit des Ziels Schaden zufügen.

- **Kalender-Einladungs-Link-Scanner**
  Diese Funktion erkennt Spam-Kalender und -Ereignisse, die gefährliche Links enthalten. Der Kalendervirus ist eine Art Spam, der die Kalender-App Ihres iPhones befällt und lästig und potenziell gefährlich sein kann:
  - Sie erhalten unerwünschte Kalendereinladungen oder Ereignisbenachrichtigungen, wenn Sie versehentlich eine gefälschte Kalendereinladung annehmen, die von Hackern oder Spammern an Ihre E-Mail-Adresse gesendet wurde.
  - Wenn Sie auf den Link in der Einladung klicken, abonnieren Sie unwissentlich den Kalender des Absenders, wodurch dieser Ihnen weitere Spam-Ereignisse senden kann.
  - Die Spam-Ereignisse können Links oder Anhänge enthalten, die Sie beim Öffnen zu Phishing-Seiten oder anderen Cyber-Bedrohungen führen könnten.

3.2.1. So richten Sie den Betrugsalarm ein

Um die Betrugswarnung zu aktivieren, müssen Sie der Bitdefender Mobile Security-App Zugriff auf Kalenderbenachrichtigungen und SMS-Nachrichten gewähren:

So aktivieren Sie die SMS-Filterung:

Damit Bitdefender mit dem Filtern von Nachrichten beginnen kann, müssen Sie die Option „Unbekannte Absender filtern“ in den Einstellungen der Nachrichten-App manuell aktivieren:

1. Öffne das **Einstellungen** App auf Ihrem iPhone oder iPad.
2. Scrollen Sie nach unten und wählen Sie aus **Mitteilungen** In der Liste.
3. Tippen Sie auf die **Unbekannt und Spam** Abschnitt.

4. Umschalten **Filtern Sie unbekannte Absender** in die Ein-Position.
5. Wählen **Mobile Sicherheit** im Abschnitt SMS-Filterung und wählen Sie dann **Aktivieren**.

Bitdefender kann jetzt Junk-Nachrichten auf Ihrem iPhone/iPad filtern.

> **Notiz**
> Aufgrund von iOS-Einschränkungen kann die Bitdefender-SMS-Filterung nur für SMS- und MMS-Nachrichten verwendet werden, die von Personen stammen, die Sie nicht in Ihren Kontakten gespeichert haben. Das bedeutet, dass Nachrichten von Personen, die sich bereits in Ihrer Kontaktliste befinden, und iMessage-Nachrichten von niemandem gefiltert werden.

So aktivieren Sie den Kalender-Scan:

1. Öffne das **Bitdefender Mobile Security** App auf Ihrem iPhone oder iPad installiert.
2. Gehe zum **Betrugsalarm** Option in der unteren Navigationsleiste und drücken Sie **Jetzt einrichten**.
3. Klopfen **Weitermachen** und tippen Sie dann auf **Aktivieren**.
4. Wählen **OK** um Bitdefender Zugriff auf Ihren Kalender zu gewähren. Ein Kalenderscan beginnt sofort.

3.3. Internet-Schutz

Der Bitdefender-Internet-Schutz lässt Sie sicher im Netz surfen, indem es Sie vor potenziell schädlichen Webseiten warnt und Sie darauf hinweist, wenn weniger sichere installierte Apps versuchen, auf nicht vertrauenswürdige Domains zuzugreifen.

Wenn eine URL auf eine bekannte Phishing-Seite oder betrügerische Website oder auf schädliche Inhalte wie Spyware oder Viren verweist, wird die Webseite blockiert und eine Warnung angezeigt.

> **Wichtig**
> Wenn Sie sich in einer Region befinden, in dem die Nutzung eines VPN-Dienstes gesetzlich eingeschränkt ist, ist der Internet-Schutz nicht verfügbar.

So können Sie den Internet-Schutz aktivieren:

1. Tippen Sie auf das Symbol {1}{2}{3}{4}{5}{6} unten auf dem Bildschirm.
2. Tippen Sie auf **Ich bin einverstanden**.
3. Aktivieren Sie den Schalter bei Internet-Schutz.

> **Notiz**
> Beim ersten Aktivieren des Internet-Schutzes werden Sie unter Umständen aufgefordert, Bitdefender die Erlaubnis zur Einrichtung der VPN-Konfiguration zur Überwachung Ihres Netzwerkdatenverkehrs zu erteilen. Tippen Sie zum Fortfahren auf **Zulassen**. Wenn Sie zum Schutz Ihres Smartphones eine Authentifizierungsmethode (Fingerabdruck oder PIN) festgelegt haben, wird diese jetzt abgefragt. Um den Aufruf nicht vertrauenswürdiger Domains erkennen zu können, nutzt der Internet-Schutz die VPN-Dienste.

> **Wichtig**
> Der Internet-Schutz und das VPN können nicht gleichzeitig genutzt werden. Sobald eines von beiden aktiviert wird, wird das andere (wenn es zu diesem Zeitpunkt aktiv ist) deaktiviert.

3.3.1. Bitdefender-Benachrichtigung

Wenn Sie versuchen, eine als unsicher eingestufte Website zu besuchen, wird die Website blockiert. Um Sie auf das Ereignis aufmerksam zu machen, werden Sie von Bitdefender in der Benachrichtigungszentrale und in Ihrem Browser benachrichtigt. Die Warnseite enthält Informationen wie die URL der Website und die erkannte Bedrohung, Sie müssen dann selbst entscheiden, wie Sie weiter vorgehen möchten.

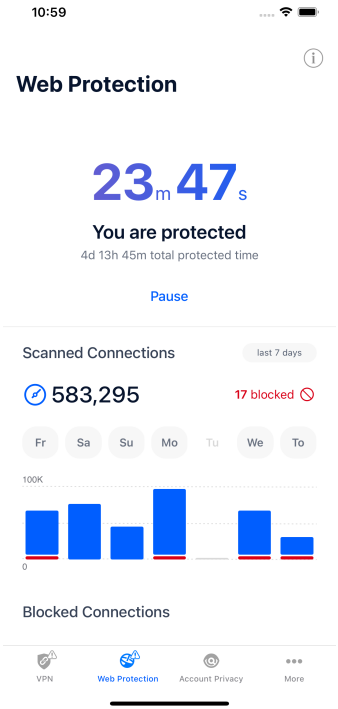
Außerdem werden Sie in der Benachrichtigungszentrale benachrichtigt, wenn eine weniger sichere App versucht, auf nicht vertrauenswürdige Domains zuzugreifen. Tippen Sie auf die angezeigte Benachrichtigung, um ein Fenster aufzurufen, in dem Sie entscheiden können, wie Sie weiter vorgehen möchten.

Die folgenden Optionen stehen für beide Fälle zur Auswahl:

- Die Website durch Tippen auf **ICH GEHE LIEBER AUF NUMMER SICHER** verlassen.

- Die Website durch Tippen auf die angezeigte Benachrichtigung und danach auf **Ich möchte die Seite aufrufen** trotz Warnung aufrufen.

Bestätigen Sie Ihre Auswahl.



3.4. VPN

Mit Bitdefender VPN schützen Sie Ihre Daten bei Verbindungen mit ungesicherten WLAN-Netzwerken wie zum Beispiel in Flughäfen, Einkaufszentren, Cafés oder Hotels. So vermeiden Sie bedauerliche Vorfälle wie den Diebstahl Ihrer persönlichen Daten oder Versuche, Ihre Geräte-IP-Adresse für Hacker offenzulegen.

Das VPN dient als Tunnel zwischen Ihrem Gerät und dem Netzwerk, mit dem Sie sich verbinden. Ihre Verbindung wird abgesichert, Ihren Daten werden professionell nach Militärstandard verschlüsselt und Ihre IP-Adresse bleibt jederzeit unsichtbar. Ihr Datenverkehr wird über einen speziellen Server weitergeleitet, was es Ihrem Provider unmöglich macht,

Ihr Gerät unter den unzähligen anderen Geräten zu identifizieren, die ebenfalls unsere Dienste in Anspruch nehmen. Darüber hinaus können Sie mit Bitdefender Mobile Security for iOS im Internet auch auf solche Inhalte zugreifen, die üblicherweise regionalen Zugangsbeschränkungen unterliegen.

> **Notiz**
> In manchen Ländern wird Internetzensur betrieben. Aus diesem Grund ist die Nutzung von VPNs hier gesetzlich verboten. Um rechtliche Konsequenzen zu vermeiden, wird Ihnen bei der ersten Nutzung der Bitdefender VPN-App eine Warnmeldung angezeigt. Durch die weitere Nutzung der App bestätigen Sie, dass Sie sich aller einschlägigen Rechtsvorschriften in Ihrem Land sowie der möglichen Risiken, denen Sie sich aussetzen, bewusst sind.

So können Sie Bitdefender VPN aktivieren:

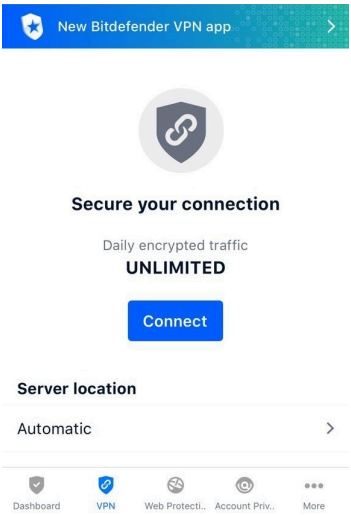
1. Tippen Sie auf die Symbol unten auf dem Bildschirm.
2. Tippen Sie auf **Verbinden**, um sich und Ihre Geräte bei Verbindungen mit ungesicherten WLAN-Netzwerken zu schützen.
   Tippen Sie auf **Trennen**, um die Verbindung wieder aufzuheben.

> **Notiz**
> Beim ersten Aktivieren des VPNs werden Sie aufgefordert, Bitdefender die Erlaubnis zur Einrichtung der VPN-Konfiguration zur Überwachung Ihres Netzwerkdatenverkehrs zu erteilen. Tippen Sie zum Fortfahren auf **Zulassen**. Wenn Sie zum Schutz Ihres Smartphones eine Authentifizierungsmethode (Fingerabdruck oder PIN) festgelegt haben, wird diese jetzt abgefragt.

Das VPN-Symbol wird bei aktivem VPN in der Statusleiste angezeigt.

Um Ihren Akku zu schonen, empfehlen wir Ihnen, VPN zu deaktivieren, wenn Sie es nicht mehr benötigen.

Falls Sie über ein Premium-Abonnement verfügen und sich mit einem Server Ihrer Wahl verbinden möchten, tippen Sie in der VPN-Benutzeroberfläche auf Automatisch und wählen Sie den gewünschten Standort aus. Weitere Details zu den VPN-Abonnements finden Sie unter Abonnements (Seite 16).



3.4.1. Abonnements

Mit Bitdefender VPN erhalten Sie ein kostenloses Datenvolumen von 200 MB pro Tag, um Ihre Verbindung bei Bedarf abzusichern. Sie werden automatisch mit dem besten Serverstandort verbunden.

Wenn Sie sich für ein Upgrade auf die Premium-Version entscheiden, entfällt das Datenlimit und Sie können durch die freie Wahl des Serverstandorts Inhaltsbeschränkungen überall auf der Welt umgehen.

Sie können jederzeit ein Upgrade auf Bitdefender Premium VPN vornehmen, indem Sie im VPN-Fenster auf **Premium VPN aktivieren** tippen. Sie können sich zwischen einem jährlichen und einem monatlichen Abonnement entscheiden.

Ein Bitdefender Premium-VPN-Abonnement läuft unabhängig von dem kostenlosen Bitdefender Mobile Security for iOS-Abonnement, d. h. Sie können es über den gesamten Verfügbarkeitszeitraum hinweg nutzen. Bei Ablauf des Bitdefender Premium-VPN-Abonnement kehren Sie automatisch zum kostenlosen Angebot zurück.

Bitdefender VPN ist plattformunabhängig und in den Windows-, macOS-, Android- und iOS-Produkten von Bitdefender verfügbar. Nach einem Premium-Upgrade können Sie Ihr Abonnement in allen Produkten nutzen, vorausgesetzt, dass Sie sich mit dem gleichen Bitdefender-Benutzerkonto anmelden.

Notiz

Bitdefender VPN ist auch als eigenständige Anwendung auf allen unterstützten Betriebssystemen einsetzbar, d. h. unter Windows, macOS, Android und iOS.

3.5. Kontoschutz

Der Bitdefender-Kontoschutz erkennt, ob die Datensicherheit der Benutzerkonten kompromittiert wurde, über die Sie Ihre Online-Zahlungen und -Einkäufe abwickeln und sich bei Ihren Apps oder Websites anmelden. Die unter Ihren Konten gespeicherten Daten umfassen Passwörter, Kreditkartendaten und Bankinformationen. Wurden diese nicht ausreichend abgesichert, kann es zu Identitätsdiebstahl und Verletzungen Ihrer Privatsphäre kommen.

Nach der Bestätigung wird der Privatsphärestatus des Benutzerkontos umgehend angezeigt.

Tippen Sie auf **Auf Datenlecks prüfen**, um zu prüfen, ob Ihre Benutzerkonten von Datenschutzverletzungen betroffen sind.

So können Sie Ihre persönlichen Daten schützen:

1. Tippen Sie auf die Symbol unten auf dem Bildschirm.
2. Tippen Sie auf **Konto hinzufügen**.
3. Geben Sie Ihre E-Mail-Adresse in das entsprechende Feld ein und tippen Sie danach auf **Weiter**.
   Bitdefender muss für dieses Konto vor der Preisgabe privater Daten erst eine Kontovalidierung durchführen. Sie erhalten zu diesem Zweck unter der angegebenen E-Mail-Adresse einen Bestätigungscode.
4. Rufen Sie Ihre E-Mails ab und geben Sie den erhaltenen Code in Ihrer App im Bereich **Kontoschutz** ein. Falls Sie Bestätigungs-E-Mail in Ihrem Posteingang nicht finden können, überprüfen Sie bitte Ihren Spam-Ordner.
   Der Privatsphärestatus des bestätigten Kontos wird angezeigt.

Wurden Datenschutzverletzungen bei einem Ihrer Benutzerkonten festgestellt, empfehlen wir Ihnen, so schnell wie möglich das entsprechende Passwort zu ändern. Mit diesen Tipps sorgen Sie für sichere Passwörter:

- Verwenden Sie mindestens acht Zeichen.
- Verwenden Sie Groß- und Kleinbuchstaben.
- Verwendenden Sie mindestens eine Zahl oder Sonderzeichen wie #, @, % oder !.

Nachdem Sie ein Konto gesichert haben, das von einer Datenpanne betroffen war, können Sie die Änderungen bestätigen, indem Sie die identifizierten Datenpannen als **Gelöst** markieren. Gehen Sie dazu wie folgt vor:

1. Tippen Sie neben der von Ihnen gelösten Datenpannen auf ···.
2. Tippen Sie auf **Als gelöst markieren**.

Wenn alle gefundenen Datenpannen als Gelöst markiert wurden, wird das Konto nicht mehr als von einer Datenpanne betroffen angezeigt, zumindest bis es zu einer weiteren Datenpanne kommt.

4. ÜBER BITDEFENDER CENTRAL

Bitdefender Central ist die Plattform, über die Sie Zugriff auf sämtliche Online-Funktionen und -Dienste des Produkts haben und über die Sie wichtige Aktionen auch per Fernzugriff auf Geräten ausführen können, auf denen Bitdefender installiert ist. Unter https://central.bitdefender.com können Sie sich von jedem mit dem Internet verbunden Computer oder Mobilgerät aus bei Ihrem Bitdefender-Konto anmelden. Auf Android- und iOS-Geräten können Sie Bitdefender Central auch über die dazugehörige App aufrufen.

So können Sie die Bitdefender-Central-App auf Ihren Geräten installieren:

- **Android** - Suchen Sie Bitdefender Central in Google Play, laden Sie die App herunter und installieren Sie sie. Folgen Sie den Anweisungen, um die Installation abzuschließen.
- **iOS** - Suchen Sie Bitdefender Central im App Store, laden Sie die App herunter und installieren Sie sie. Folgen Sie den Anweisungen, um die Installation abzuschließen.

Nachdem Sie sich angemeldet haben, stehen Ihnen die folgenden Optionen zur Verfügung:

- Laden Sie Bitdefender herunter und installieren Sie es auf Windows-, macOS-, iOS- und Android-Betriebssystemen. Die folgenden Produkte stehen zum Download bereit:
  - Bitdefender Mobile Security für iOS
  - Bitdefender Mobile Security for Android
  - Bitdefender Antivirus for Mac
  - Die Bitdefender-Produktlinie für Windows
- Verwaltung und Verlängerung Ihrer Bitdefender-Abonnements.
- Neue Geräte zu Ihrem Netzwerk hinzufügen und diese Geräte aus der Ferne verwalten.

4.1. Aufrufen von Bitdefender Central

Sie haben zwei Möglichkeiten zum Aufrufen von Bitdefender Cental

- Über Ihren Web-Browser:

1. Öffnen Sie einen Web-Browser auf jedem beliebigen internetfähigen Gerät.
2. Gehen Sie zu: https://central.bitdefender.com.
3. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Konto an.

- Über Ihr Android- oder iOS-Gerät:
  Öffnen Sie die von Ihnen installierte Bitdefender Central-App.

  Notiz
  Hier finden Sie alle Optionen, die Ihnen über die Web-Oberfläche zur Verfügung gestellt werden.

4.2. Zwei-Faktor-Authentifzierung

Die Zwei-Faktor-Authentifizierung fügt Ihrem Bitdefender-Benutzerkonto eine weitere Sicherheitsebene hinzu, indem sie zusätzlich zu Ihren Anmeldeinformationen einen Authentifizierungscode anfordert. Auf diese Weise verhindern Sie unbefugten Zugriff auf Ihr Benutzerkonto und schützen sich vor Cyberangriffen wie Keylogger-, Brute-Force- oder Wörterbuchangriffen.

4.2.1. Aktivieren der Zwei-Faktor-Authentifizierung

Durch die Aktivierung der Zwei-Faktor-Authentifizierung wird Ihr Bitdefender-Benutzerkonto deutlich besser abgesichert. Sie müssen Ihre Identität für jede Anmeldung über ein neues Gerät erneut bestätigen, so zum Beispiel wenn Sie eines der Bitdefender-Produkte installieren, Ihren Abonnementstatus einsehen oder per Fernzugriff Aufgaben auf Ihren Geräten ausführen.

So aktivieren Sie die Zwei-Faktor-Authentifizierung:

1. Zugang Bitdefender-Zentrale.
2. Tippen Sie oben rechts auf dem Bildschirm auf das Symbol {1}{2}{3}{4}{5}{6}.
3. Tippen Sie im Schiebemenü auf {1}Bitdefender-Konto{2}.
4. Wechseln Sie zum Reiter {1}Passwort und Sicherheit{2}.
5. Tippen Sie auf **ERSTE SCHRITTE**.
   Wählen Sie eine der folgenden Methoden aus:

- **Authentifizierungsanwendung** - Verwenden Sie eine Authentifizierungsanwendung, um für jede Anmeldung bei Ihrem Bitdefender-Konto einen Code zu generieren.
  Wenn Sie eine Authentifizierungsanwendung verwenden möchten, sich aber nicht sicher sind, welche App Sie verwenden sollen, können Sie sie aus einer Liste mit den von uns empfohlenen Authentifizierungsanwendung auswählen.

  a. Tippen Sie zunächst auf **AUTHENTIFIZIERUNGSANWENDUNG VERWENDEN**.

  b. Verwenden Sie zur Anmeldung auf einem Android- oder iOS-Gerät Ihr Gerät, um den QR-Code zu scannen.
  Zur Anmeldung auf einem Laptop oder Computer können Sie den angezeigten Code manuell eingeben.
  Tippen Sie auf **Fortfahren**

  c. Geben Sie den von der App generierten bzw. den im vorherigen Schritt angezeigten Code ein, und tippen Sie dann auf **AKTIVIEREN**.

- **E-Mail** - Bei jeder Anmeldung an Ihrem Bitdefender-Konto wird ein Bestätigungscode an Ihre E-Mail-Adresse gesendet. Rufen Sie Ihre E-Mails ab und verwenden Sie den erhaltenen Code.

  a. Tippen Sie zunächst auf **E-MAIL VERWENDEN**.

  b. Rufen Sie Ihre E-Mails ab, und geben Sie den erhaltenen Code ein.
  Bitte beachten Sie, dass Sie fünf Minuten Zeit haben, Ihre E-Mails abzurufen und den generierten Code einzugeben. Nach Ablauf dieser Zeit müssen Sie einen neuen Code generieren, indem Sie die gleichen Schritte erneut ausführen.

  c. Tippen Sie auf **AKTIVIEREN**.

  d. Sie erhalten zehn Aktivierungscodes. Sie können die Liste entweder kopieren, herunterladen oder ausdrucken und für den Fall verwenden, dass Sie Ihre E-Mail-Adresse verlieren oder sich nicht mehr anmelden können. Jeder Code kann nur einmal verwendet werden.

  e. Tippen Sie auf **FERTIG**.

Gehen Sie folgendermaßen vor, wenn Sie die Zwei-Faktor-Authentifizierung nicht mehr nutzen möchten:

1. Tippen Sie auf **ZWEI-FAKTOR-AUTHENTIFIZIERUNG DEAKTIVIEREN**.
2. Sehen Sie in die App oder rufen Sie Ihre E-Mails ab, und geben Sie den erhaltenen Code ein.
   Falls Sie sich für den Empfang des Authentifizierungscodes per E-Mail entschieden haben, haben Sie fünf Minuten Zeit, um Ihre E-Mails abzurufen und den generierten Code einzugeben. Nach Ablauf dieser Zeit müssen Sie einen neuen Code generieren, indem Sie die gleichen Schritte erneut ausführen.
3. Bestätigen Sie Ihre Auswahl.

4.3. Hinzufügen vertrauenswürdiger Geräte

Um sicherzustellen, dass nur Sie auf Ihr Bitdefender-Konto zugreifen können, fragen wir unter Umständen zunächst einen Sicherheitscode ab. Wenn Sie bei Anmeldungen über das gleiche Gerät diesen Schritt überspringen möchten, empfehlen wir, dass Sie ein vertrauenswürdiges Gerät festzulegen.

So können Sie Geräte als vertrauenswürdige Geräte festlegen:

1. Zugang Bitdefender-Zentrale.
2. Tippen Sie auf die Symbol oben rechts auf dem Bildschirm.
3. Klopfen **Bitdefender-Konto** im Folienmenü.
4. Wähle aus **Passwort und Sicherheit** Tab.
5. Tippen Sie auf **Vertrauenswürdige Geräte**.
6. Es wird eine Liste mit Geräten angezeigt, auf denen Bitdefender installiert ist. Tippen Sie auf das gewünschte Gerät.

Sie können beliebig viele Geräte hinzufügen, vorausgesetzt, dass Bitdefender auf ihnen installiert ist und Sie über ein gültiges Abonnement verfügen.

4.4. Meine Geräte

Über Ihr Bitdefender-Benutzerkonto können Sie im Bereich **Meine Geräte** die Bitdefender-Produkte auf Ihren Geräten aus der Ferne

installieren und verwalten, sofern die Geräte eingeschaltet und mit dem Internet verbunden sind. Auf den Gerätekacheln sind der Gerätename, der Sicherheitsstatus angegeben sowie die Information, ob Sicherheitsprobleme auf Ihren Geräten bestehen.

4.4.1. Hinzufügen eines neuen Geräts

Falls Ihr Abonnement mehr als ein Gerät umfasst, können Sie ein neues Gerät hinzufügen und darauf Ihr Bitdefender Mobile Security for iOS installieren. Gehen Sie dazu wie folgt vor:

1. Zugang Bitdefender Central.
2. Wähle aus **Meine Geräte** Bedienfeld und tippen Sie dann auf **SCHUTZ INSTALLIEREN**.
3. Wählen Sie eine der beiden verfügbaren Optionen:
   - **Schützen Sie dieses Gerät**
     Wählen Sie diese Option und dann den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, tippen Sie auf die entsprechende Schaltfläche.
   - **Schützen Sie andere Geräte**
     Wählen Sie diese Option und dann den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, tippen Sie auf die entsprechende Schaltfläche.
     Klicken Sie auf **DOWNLOAD LINK SENDEN**. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **E-MAIL VERSENDEN**. Bitte beachten Sie, dass der generierte Download-Link nur für die nächsten 24 Stunden gültig ist. Nach Ablauf des Links müssen Sie einen neuen Link generieren. Führen Sie dazu die bereits beschriebenen Schritte erneut aus.
     Überprüfen Sie auf dem Gerät, auf dem Sie Ihr Bitdefender-Produkt installieren möchten, das E-Mail-Konto, das Sie eingegeben haben, und tippen Sie dann auf die entsprechende Download-Schaltfläche.
4. Warten Sie, bis der Download abgeschlossen ist, und führen Sie das Installationsprogramm aus.

4.4.2. Persönliche Anpassungen

Sie können Gerätenamen vergeben, um die Geräte später leichter identifizieren zu können:

1. Zugang Bitdefender Central.
2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie auf die gewünschte Gerätekachel und dann auf das Symbol ⋮ in der rechten oberen Ecke.
4. Wählen Sie **Einstellungen**.
5. Geben Sie einen neuen Namen in das Feld **Gerätename** ein und klicken Sie dann auf **SPEICHERN**.

Sie können für jedes Ihrer Geräte zur einfacheren Verwaltung einen Besitzer anlegen und zuordnen:

1. Zugang Bitdefender Central.
2. Wähle aus **Meine Geräte** Tafel.
3. Tippen Sie auf die gewünschte Gerätekarte und dann auf ⋮ Symbol in der oberen rechten Ecke des Bildschirms.
4. Wählen Sie **Profil**.
5. Klicken Sie auf **Besitzer hinzufügen** und füllen Sie im Anschluss die entsprechenden Felder aus. Passen Sie das Profil nach Bedarf an, indem Sie ein Foto hinzufügen, einen Geburtstag auswählen und eine E-Mail-Adresse sowie eine Telefonnummer eingeben.
6. Klicken Sie auf **HINZUFÜGEN**, um das Profil zu speichern.
7. Wählen Sie aus der Liste der **Gerätebesitzer** den gewünschten Besitzer aus und klicken Sie auf **ZUORDNEN**.

4.4.3. Fernzugriffsaktionen

So können Sie Bitdefender per Fernzugriff auf Ihren Geräten aktualisieren:

1. Zugang Bitdefender Central.
2. Wähle aus **Meine Geräte** Tafel.
3. Tippen Sie auf die gewünschte Gerätekarte und dann auf ⋮ Symbol in der oberen rechten Ecke des Bildschirms.

4. Wählen Sie **Update**.

Klicken Sie auf die entsprechende Gerätekarte, um das Gerät per Fernzugriff zu steuern oder Informationen zu Ihrem Bitdefender-Produkt auf einem bestimmten Geräte anzuzeigen.

Klicken Sie auf eine Gerätekarte, um die folgenden Reiter anzuzeigen:

- **Dashboard.** In diesem Fenster werden Details zum ausgewählten Gerät angezeigt sowie sein Sicherheitsstatus, der Status des Bitdefender VPN und wie viele Bedrohungen in den vergangenen 7 Tagen blockiert wurden. Der Sicherheitsstatus ist grün, wenn es keine Sicherheitsprobleme gibt, gelb, wenn es etwas gibt, was Ihre Aufmerksamkeit erfordert, und rot, wenn Ihr Gerät gefährdet ist. Wenn Probleme bestehen, klicken Sie auf das Klappmenü oben im Statusbereich, um mehr Details dazu anzuzeigen. Hier können Sie
- **Schutz.** Von diesem Fenster aus können Sie Quick- und System-Scans auf Ihrem Gerät durchführen. Klicken Sie dazu auf die Schaltfläche **SCANNEN**. Hier können Sie auch einsehen, wann der letzte Scan auf dem Gerät durchgeführt wurde, und einen Bericht mit den wichtigsten Informationen zum letzten Scan aufrufen.
- **Optimierung.** Hier können Sie per Fernzugriff die Leistung eines Geräts verbessern, indem Sie nicht mehr benötigte Dateien schnell und einfach aufspüren und entfernen. Klicken Sie auf **START** und wählen Sie dann die Bereiche aus, die Sie optimieren möchten. Klicken Sie erneut auf **START**, um den Optimierungsvorgang zu starten. Klicken Sie auf **Weitere Details**, um einen detaillierten Bericht mit Informationen zu den behobenen Probleme aufzurufen.
- **Diebstahlschutz.** Falls Sie Ihr Gerät verlegen oder verlieren oder sollte es gestohlen werden, hilft Ihnen die Diebstahlschutzfunktion Ihr Gerät zu orten und per Fernzugriff bestimmte Aktionen durchzuführen. Klicken Sie auf **ORTEN**, um den Standort des Geräts zu ermitteln. Der letzte bekannte Standort wird zusammen mit Uhrzeit und Datum angezeigt.
- **Schwachstelle**. Um ein Gerät auf Schwachstellen wie fehlende Windows-Updates, veraltete Anwendungen oder unsichere Passwörter zu überprüfen, klicken Sie im Reiter Schwachstellen auf **SCANNEN**. Schwachstellen können nicht per Fernzugriff behoben werden. Falls eine Schwachstelle gefunden wird, müssen Sie einen erneuen Scan auf dem Gerät durchführen und dann die empfohlenen Maßnahmen

ergreifen. Klicken Sie auf **Weitere Details**, um einen detaillierten Bericht über die gefundenen Probleme aufzurufen.

4.5. Aktivität

Im Bereich Aktivität können Sie Informationen zu den Geräten einsehen, auf denen Bitdefender installiert ist.

Im Fenster **Aktivität** können Sie auf die folgenden Kacheln zugreifen:

- **Meine Geräte.** Hier können Sie die Anzahl der verbundenen Geräte sowie ihren jeweiligen Schutzstatus anzeigen. Um per Fernzugriff Probleme auf den erkannten Geräten zu beheben, klicken Sie auf **Probleme beheben** und dann auf **SCANNEN UND PROBLEME BEHEBEN**.
  Um Details zu den erkannten Problemen anzuzeigen, klicken Sie auf **Probleme anzeigen**.
  Von iOS-Geräten können keine Informationen zu erkannten Bedrohungen abgerufen werden.
- **Bedrohungen blockiert.** Hier können Sie ein Diagramm mit einer Gesamtstatistik mit Informationen über die blockierten Bedrohungen der letzten 24 Stunden bzw. 7 Tage anzeigen. Die angezeigten Informationen werden abhängig von dem schädlichen Verhalten abgerufen, das bei den aufgerufenen Dateien, Anwendungen und URLs erkannt wurde.
- **Benutzer mit den meisten blockierten Bedrohungen.** Hier können Sie eine Übersicht mit den Anwendern anzeigen, bei denen die meisten Bedrohungen gefunden wurden.
- **Geräte mit den meisten blockierten Bedrohungen.** Hier können Sie eine Übersicht mit den Geräten anzeigen, auf denen die meisten Bedrohungen gefunden wurden.

4.6. Meine Abonnements

Über die Bitdefender Central-Plattform können Sie bequem die Abonnements für alle Ihre Geräte verwalten.

4.6.1. Verfügbare Abonnements anzeigen

So können Sie Ihre verfügbaren Abonnements anzeigen:

1. Zugang Bitdefender Central.
2. Rufen Sie den Bereich **Meine Abonnements** auf.

Hier werden alle Informationen zur Verfügbarkeit Ihrer Abonnements und die Anzahl der Geräte angezeigt, auf denen diese verwendet werden.

Klicken Sie auf eine Abonnementkarte, um Ihrem Abonnement ein neues Gerät hinzuzufügen oder es zu verlängern.

> **Hinweis**
> Es ist möglich, eine oder mehrere Abonnements unter einem Benutzerkonto zu vereinen, vorausgesetzt, dass diese für verschiedene Plattformen (Windows, macOS, iOS oder Android) gültig sind.

4.6.2. Abonnement aktivieren

Sie können ein Abonnement während des Installationsvorgangs mithilfe Ihres Bitdefender-Kontos aktivieren. Sobald die Aktivierung abgeschlossen ist, beginnt die Laufzeit des Abonnements.

Falls Sie einen Aktivierungscode von einem unserer Wiederverkäufer gekauft oder diesen als Geschenk erhalten haben, können Sie die Gültigkeitsdauer Ihres Bitdefender-Abonnements um diesen Zeitraum verlängern.

So können Sie Ihr Abonnement mit einem Aktivierungscode aktivieren:

1. Zugang Bitdefender Central.
2. Wähle aus **Meine Abonnements** Tafel.
3. Klicken Sie auf **AKTIVIERUNGSCODE** und geben Sie den Code in das entsprechende Feld ein.
4. 2Klicken Sie zum Fortfahren auf **AKTIVIEREN**.

Das Abonnement wurde aktiviert.

4.6.3. Abonnement verlängern

Falls Sie die automatische Verlängerung Ihres Bitdefender-Abonnements deaktiviert haben, können Sie es auch selbst verlängern. Gehen Sie dazu wie folgt vor:

1. Zugang Bitdefender Central.
2. Wähle aus **Meine Abonnements** Tafel.

3. Wählen Sie die gewünschte Abonnementkarte aus.
4. Klicken Sie zum Fortfahren auf **VERLÄNGERN**.

In Ihrem Web-Browser wird eine neue Seite geöffnet, über die Sie Ihr Bitdefender-Abonnement verlängern können.

4.7. Benachrichtigungen

Über das -Symbol bleiben Sie immer auf dem Laufenden, was auf den mit Ihrem Konto verbundenen Geräten passiert. Ein Klick auf dieses Symbol gibt Ihnen einen groben Überblick über die Aktivitäten der Bitdefender-Produkte, die auf Ihren Geräten installiert sind.

5. HÄUFIG GESTELLTE FRAGEN

Wie schützt mich Bitdefender Mobile Security for iOS vor Viren und Cyberbedrohungen?

Bitdefender Mobile Security for iOS bietet absoluten Schutz vor allen Cyberbedrohungen und wurde eigens entwickelt, um Ihre sensiblen Daten vor neugierigen Augen zu schützen.

Sie erhalten eine Vielzahl an leistungsfähigen Sicherheits- und Datenschutzfunktionen für Ihr iPhone oder iPad - und dazu Bonusfunktionen, einschließlich VPN und Internet-Schutz.

Bitdefender Mobile Security for iOS reagiert umgehend auf Viren und Malware, ohne die Leistung Ihres Systems zu beeinträchtigen.

Für welche Geräte und Betriebssysteme ist Bitdefender Mobile Security for iOS geeignet?

Bitdefender Mobile Security for iOS schützt Ihre unter iOS laufenden Smartphones und Tablets vor allen Cyberbedrohungen.

Warum benötige ich Bitdefender Mobile Security for iOS auf Computern mit Apple OS?

Auf Ihrem iPhone oder iPad sind sehr persönliche Daten gespeichert. Da müssen sich jederzeit darauf verlassen können, dass diese Daten geschützt sind. Mit Bitdefender Mobile Security for iOS sind Sie absolut sicher vor Cyberbedrohungen und brauchen sich keine Gedanken um den Schutz Ihrer privaten Daten zu machen, wenn Sie online sind, ohne dass Ihre täglichen Aktivitäten im Internet dadurch behindert werden.

Erhalte ich mit meinen Bitdefender Mobile Security for iOS-Abonnement auch ein VPN?

Bitdefender Mobile Security for iOS beinhaltet eine Basisversion von Bitdefender VPN inkl. kostenlosem großzügigem Datenvolumen (200 MB pro Tag, 6 GB pro Monat).

6. HILFE UND SUPPORT

6.1. Hier wird Ihnen geholfen

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

6.2. Online-Ressourcen

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

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

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

6.2.1. Bitdefender-Support-Center

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

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

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

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

6.2.2. Die Bitdefender Experten Community

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

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

Hier geht's zur Website unserer Expert Community:

https://community.bitdefender.com/de

6.2.3. Bitdefender Cyberpedia

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

Die Bitdefender Cyberpedia finden Sie hier:

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

6.3. Kontaktinformation

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

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

6.3.1. Lokale Vertriebspartner

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

So finden Sie einen Bitdefender Distributor in Ihrem Land:

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

GLOSSAR

Aktivierungscode

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

ActiveX

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

Advanced Persistent Threat

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

Adware

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

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

Archiv

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

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

Hintertür

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

Bootsektor

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

Bootvirus

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

Botnet

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

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

Browser

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

Brute-Force-Angriff

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

Befehlszeile

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

Cookies

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

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

Cybermobbing

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

Wörterbuchangriff

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

Laufwerk

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

Download

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

E-Mail

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

Ereignisse

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

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

Exploits

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

Fehlalarme

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

Dateinamenerweiterung

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

Heuristik

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

Honeypot

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

IP

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

Java-Applet

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

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

Keylogger

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

Makrovirus

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

Mail-Client

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

Arbeitsspeicher

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

Nicht-heuristisch

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

Online-Missbrauch

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

Komprimierte Programme

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

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

Pfad

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

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

Phishing

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

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

Photon

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

Polymorphic virus

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

Port

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

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

Ransomware

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

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

Berichtsdatei

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

Rootkit

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

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

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

Skript

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

Spam

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

Spyware

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

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

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

Systemstartelemente

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

Abonnement

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

Taskleiste

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

TCP/IP

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

Bedrohung

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

Update der Bedrohungsinformationen

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

Trojaner

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

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

Update

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

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

Virtual Private Network (VPN)

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

Wurm

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