Bitdefender ANTIVIRUS FREE

BENUTZERHANDBUCH

Bitdefender Antivirus Free
Benutzerhandbuch

Veröffentlicht 27.04.2022

Rechtlicher Hinweis

Bitdefender

Inhaltsverzeichnis

INSTALLATION

1. VOR DER INSTALLATION

Bevor Sie Bitdefender Antivirus Free installieren, sollten Sie für eine reibungslose Installation sicherstellen, dass folgende Schritte durchgeführt wurden:

- Stellen Sie sicher, dass das Zielgerät für die Bitdefender-Installation die Systemvoraussetzungen erfüllt. Wenn das Gerät die Systemvoraussetzungen nicht erfüllt, kann Bitdefender nicht installiert werden. Falls es doch installiert wird, kann es zu Leistungseinbußen und Stabilitätsproblemen kommen. Eine vollständige Liste der Systemanforderungen finden Sie im Kapitel *„Systemanforderungen“* (S. 3).
- Melden Sie sich mit einem Administrator-Konto am Gerät an.
- Entfernen Sie alle anderen Sicherheitslösungen von Ihrem Gerät. Sollte während des Bitdefender-Installationsvorgangs welche gefunden werden, werden Sie aufgefordert, sie zu deinstallieren. Die gleichzeitige Nutzung mehrerer Sicherheitsprogramme kann die jeweilige Funktion stören und massive Probleme auf Ihrem Computer verursachen. Windows Defender wird während der Installation deaktiviert.

2. SYSTEMANFORDERUNGEN

Sie können Bitdefender Antivirus Free nur auf Geräten mit den folgenden Betriebssystemen installieren:

- Windows 7 mit Service Pack 1
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

- 2,5 GB verfügbarer Festplattenspeicher (davon mindestens 800 MB auf dem Systemlaufwerk)
- 2 GB Arbeitsspeicher (RAM)
- An active internet connection

Wichtig
Die Systemleistung kann auf Geräten mit CPUs der alten Generation beeinträchtigt werden.

Beachten Sie
So können Sie Informationen zu Ihrem Windows-Betriebssystem und Ihrer Hardware finden:

- Rechtsklicken Sie unter **Windows 7** im Desktop auf **Arbeitsplatz** und wählen Sie **Eigenschaften** aus dem Menü.
- In **Windows 8**, finden Sie auf der Windows-Startseite den Eintrag **Computer**(z.B. durch die Eingabe von "Computer" auf der Startseite) und klicken Sie auf das entsprechende Symbol. Finden Sie unter **Windows 8.1 Dieser PC**.

  Wählen Sie im Menü unten **Eigenschaften**. Im Bereich **System** finden Sie Informationen zu Ihrem Systemtyp.
- Geben Sie unter **Windows 10 System** in das Suchfeld in der Taskleiste ein und klicken Sie auf das entsprechende Symbol. Im Bereich **System** finden Sie Informationen zu Ihrem Systemtyp.

2.1. Software-Anforderungen

Um Bitdefender und alle Funktionen nutzen zu können, muss Ihr Gerät die folgenden Software-Anforderungen erfüllen:

- Ab Microsoft Edge 40

- Internet Explorer 11 und höher
- Mozilla Firefox 51 und höher
- Google Chrome 34 und höher

3. INSTALLIEREN IHRES BITDEFENDER-PRODUKTS

You can install Bitdefenderusing the web installer downloaded on your device from the Bitdefender Antivirus Free page on Bitdefender Website.

3.1. Install from Bitdefender Website

From Bitdefender Website you can download the Bitdefender Antivirus Free installation kit. Once the installation process is complete, Bitdefender Antivirus Free is activated.

To download Bitdefender Antivirus Free from Bitdefender Website:

1. Access https://www.bitdefender.com/toolbox/ .
2. Click download on Bitdefender Antivirus Free.
3. Warten Sie, bis der Download abgeschlossen ist, und führen Sie das Installationsprogramm aus.

Validierung der Installation

Bitdefender wird zuallererst Ihr System überprüfen, um die Installation zu bestätigen.

Wenn Ihr System die Systemvoraussetzungen zur Installation von Bitdefender nicht erfüllt, werden Sie darüber informiert, welche Bereiche aufgerüstet werden müssen, damit Sie fortfahren können.

Wenn eine inkompatible Sicherheitslösung oder eine ältere Version von Bitdefender erkannt wird, werden Sie aufgefordert, diese von Ihrem System zu entfernen. Bitte folgen Sie den Anweisungen, um die Software von Ihrem System zu entfernen und so spätere Probleme zu vermeiden. Unter Umständen müssen Sie Ihr Gerät neu starten, um die Entfernung der erkannten Sicherheitslösungen abzuschließen.

Das Installationspaket für Bitdefender Antivirus Free wird ständig aktualisiert.

Beachten Sie
Das Herunterladen der Installationsdateien kann eine Weile dauern, besonders bei langsameren Internetverbindungen.

Sobald die Installation validiert ist, startet der Installationsassistent. Folgen Sie den Schritten, um Bitdefender Antivirus Free auf Ihrem PC zu installieren.

Schritt 1 - Installation von Bitdefender

Bevor Sie mit Installation fortfahren 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 Antivirus Free nutzen dürfen.

Sollten Sie diesen Nutzungsbedingungen nicht zustimmen, schließen Sie das Fenster. Der Installationsprozess wird abgebrochen uns Sie verlassen den Assistenten.

In diesem Schritt können Sie zwei zusätzliche Dinge tun:

- Lassen Sie die Option **Produktberichte senden** aktiviert. Bleibt diese Option aktiviert, werden Berichte mit Informationen über Ihre Nutzung des Produkts an die Bitdefender-Server übertragen. Diese Information ist wichtig für die Verbesserung des Produktes. Wir möchten Sie darauf hinweisen, dass diese Berichte keine vertraulichen Daten wie Ihren Namen oder Ihre IP-Adresse enthalten und dass diese Daten nicht für kommerzielle Zwecke verwendet werden.
- Wählen Sie die Sprache aus, in der das Produkt installiert werden soll.

Klicken Sie auf **INSTALLIEREN**, um den Installationsvorgang für Ihr Bitdefender-Produkt zu starten.

Schritt 2 - Installation wird durchgeführt

Bitte warten Sie, bis der Installationsvorgang abgeschlossen ist. Sie erhalten detaillierte Informationen über den Fortschritt der Installation.

Schritt 3 - Installation ist abgeschlossen

Ihr Bitdefender-Produkt wurde erfolgreich installiert.

Eine Zusammenfassung der Installation wird angezeigt. Sollte während der Installation aktive Bedrohungen erkannt und entfernt werden, könnte ein Neustart des Systems erforderlich werden.

Schritt 4 - Geräteanalyse

Sie werden jetzt gefragt, ob Sie eine Analyse Ihres Geräts durchführen möchten, um sicherzustellen, dass es nicht gefährdet ist. In diesem Schritt

wird Bitdefender kritische Systembereiche scannen. Klicken Sie zum Starten auf **Geräteanalyse starten**.

Sie können die Scan-Oberfläche ausblenden, indem Sie auf **Scan im Hintergrund ausführen** klicken. Legen Sie danach fest, ob Sie informiert werden möchten, wenn der Scan abgeschlossen ist.

Klicken Sie nach Abschluss des Scans auf **Bitdefender-Benutzerkonto anlegen**.

Beachten Sie
Alternativ können Sie, wenn Sie den Scan nicht durchführen möchten, einfach auf **Überspringen** klicken.

Schritt 5 - Bitdefender-Konto

Nach Abschluss der Ersteinrichtung wird das Bitdefender-Konto-Fenster angezeigt. Zur Aktivierung des Produktes und zur Nutzung seiner Online-Funktionen wird ein Bitdefender-Benutzerkonto benötigt. Weitere Informationen finden Sie im Kapitel *„Bitdefender Central“* (S. 23).

Fahren Sie entsprechend Ihrer Situation fort.

- **Ich möchte ein Bitdefender-Konto anlegen**

  1. Geben Sie die Daten in die entsprechenden Felder ein. Die hier eingetragenen Daten bleiben vertraulich. Das Passwort muss mindestens 8 Zeichen enthalten, davon mindestens eine Ziffer, ein Sonderzeichen, einen Kleinbuchstaben und einen Großbuchstaben.
  2. Bevor Sie fortfahren können, müssen Sie zunächst den Nutzungsbedingungen zustimmen. Rufen Sie die Nutzungsbedingungen auf und lesen Sie sie aufmerksam durch, da Sie hier die Bedingungen zur Nutzung von Bitdefender finden.

     Darüber hinaus können Sie auch die Datenschutzrichtlinie aufrufen und lesen.
  3. Klicken Sie auf **KONTO ERSTELLEN**.

Beachten Sie
Sobald das Benutzerkonto erstellt wurde, können Sie sich mit der angegebenen E-Mail-Adresse und dem Passwort unter https://central.bitdefender.com bei Ihrem Konto anmelden. Alternativ ist dies auch über die Bitdefender Central-App möglich, falls Sie diese auf

einem Ihrer Android- oder iOS-Geräten installiert haben. Rufen Sie zur Installation der Bitdefender Central-App auf Ihrem Android-Gerät Google Play auf, suchen Sie Bitdefender Central und tippen Sie auf Installieren. Rufen Sie zur Installation der Bitdefender Central-App auf Ihrem iOS-Gerät den App Store auf, suchen Sie Bitdefender Central und tippen Sie auf Installieren.

- **Ich habe bereits ein Bitdefender Benutzerkonto.**

  1. Klicken Sie auf **Anmelden**.
  2. Geben Sie die E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **WEITER**.
  3. Geben Sie Ihr Passwort ein und klicken Sie auf **ANMELDEN**.

     Wenn Sie das Passwort vergessen haben oder aus anderen Gründen zurücksetzen möchten, gehen Sie bitte wie folgt vor:

     a. Klicken Sie auf **Passwort vergessen?**.

     b. Geben Sie Ihre E-Mail-Adresse ein und klicken Sie auf **WEITER**.

     c. Rufen Sie Ihre E-Mails ab, geben Sie den Sicherheitscode ein, den Sie per E-Mail bekommen haben, und klicken Sie auf **WEITER**.

        Oder Sie klicken in der E-Mail, die Sie von uns bekommen haben, auf **Passwort ändern**.

     d. Geben Sie Ihre gewünschtes neues Passwort ein. Geben Sie es dann noch ein zweites Mal ein. Klicken Sie auf **SPEICHERN**.

     Beachten Sie
     Falls Sie bereits über ein MyBitdefender-Benutzerkonto verfügen, können Sie sich mit den Zugangsdaten bei Bitdefender-Konto anmelden. Falls Sie Ihr Passwort vergessen haben, müssen Sie es unter https://my.bitdefender.com zunächst zurücksetzen. Verwenden Sie danach die aktualisierten Zugangsdaten, um sich bei Ihrem Bitdefender-Konto anzumelden.

- **Ich möchte mich über mein Microsoft-, Facebook- oder Google-Konto anmelden**

  So können Sie sich mit Ihrem Microsoft-, Facebook- oder Google-Konto anmelden:

1. Wählen Sie, worüber Sie sich anmelden möchten. Sie werden auf die Anmeldeseite dieses Dienstes weitergeleitet.
2. Folgen Sie den Anweisungen des ausgewählten Dienstes, um Ihr Benutzerkonto mit Bitdefender zu verknüpfen.

Beachten Sie
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.

Schritt 6 - Produkt aktivieren

Beachten Sie
Dieser Schritt muss durchgeführt werden, falls Sie sich im vorausgegangenem Schritt für die Anlage eines neuen Bitdefender-Konto entschieden haben oder sich mit einem Benutzerkonto angemeldet haben, für das das Abonnement bereits abgelaufen ist.

Zum Abschluss der Produktaktivierung wird eine aktive Internet-Verbindung benötigt.

If you already have an active subscription on your account, that subscription will be used to protect your device.

If you do not have an active subscription, your Bitdefender Antivirus Free will be activated. You can also opt-in for a 30 days Bitdefender Total Security trial.

Schritt 7 - Erste Schritte

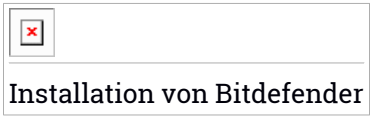
Im Fenster **Erste Schritte** erhalten Sie erweiterte Informationen zu Ihrem aktivem Abonnement.

Klicken Sie auf **BEENDEN**, um die Bitdefender Antivirus Free-Benutzeroberfläche aufzurufen.

3.2. Über vorhandene Sicherheitslösungen installieren

Der Einsatz mehrerer Sicherheitslösungen auf Ihrem Gerät kann zu Fehlfunktionen wie Systemverlangsamungen oder Abstürzen führen.

Um sicherzustellen, dass Ihr Gerät nicht durch die Verwendung mehrerer Sicherheitslösungen beeinträchtigt wird, führt Sie Bitdefender Antivirus Free während des Installationsvorgangs durch die Deinstallation der erkannten vorhandenen Sicherheitslösungen.



INBETRIEBNAHME

4. BITDEFENDER-BENUTZEROBERFLÄCHE

Bitdefender Antivirus Free entspricht den Bedürfnissen sowohl von Profis als auch von Beginnern. Die grafische Benutzeroberfläche ist so konzipiert, dass Sie für jeden Benutzer anpassbar ist.

Oben links wird ein Assistent eingeblendet, der Sie durch die Elemente der Bitdefender-Oberfläche leitet und Ihnen bei der Konfiguration zur Seite steht. Klicken Sie auf die Spitze Klammer rechts, um dem Assistenten weiter zu folgen, oder **Einführung überspringen**, um den Assistenten zu schließen.

Über das Bitdefender-Taskleistensymbol können Sie jederzeit das Hauptfenster öffnen, ein Produktupdate durchführen oder Informationen zur installierten Version abrufen.

Im Hauptfenster finden Sie Informationen zu Ihren Sicherheitsstatus. Abhängig von Ihrer Gerätenutzung und Ihren Anforderungen, zeigt der Autopilot hier unterschiedliche Empfehlungen an, um Sie bei der Verbesserung Ihrer Gerätesicherheit und -leistung zu unterstützen. Sie können darüber hinaus Schnellaktionen für die von Ihnen am häufigsten genutzten Funktionen hinzufügen, damit Sie jederzeit darauf zugreifen können.

Über das Navigationsmenü links können Sie auf die Einstellungen, die Benachrichtigungen und die verschiedenen Bitdefender-Bereiche zugreifen, um das Produkt im Detail zu konfigurieren und auf erweiterte Administrationsaufgaben zuzugreifen.

Über den Bereich oben im Hauptfenster können Sie auf Ihr Bitdefender-Benutzerkonto zugreifen. Sie können auch jederzeit unseren Support kontaktieren, falls Sie noch Fragen haben oder unerwartete Probleme auftreten.

Wenn Sie wichtige Sicherheitsinformationen ständig im Blick haben und direkten Zugriff auf wichtige Einstellungen haben möchten, können Sie das Sicherheits-Widget zu Ihrem Desktop hinzufügen.

4.1. Task-Leisten-Symbol

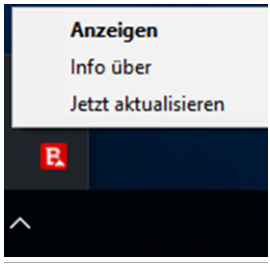
Um das gesamte Produkt schneller zu verwalten, können Sie das Bitdefender-Symbol in der Task-Leiste nutzen.

Beachten Sie

Das Bitdefender-Symbol ist unter Umständen nicht immer sichtbar. So können Sie das Symbol dauerhaft anzeigen lassen:

- In **Windows 7, Windows 8 und Windows 8.1**:
  1. Klicken Sie auf den Pfeil in der unteren rechten Ecke des Bildschirms.
  2. Klicken Sie auf **Benutzerdefiniert ...**, um das Fenster der Infobereichsymbole zu öffnen.
  3. Wählen Sie **Symbole und Benachrichtigungen anzeigen** für das Symbol **Bitdefender Agent**.
- In **Windows 10**:
  1. Klicken Sie mit der rechten Maustaste auf die Taskleiste und wählen Sie **Taskleisteneinstellungen**.
  2. Scrollen Sie nach unten und klicken Sie unter **Infobereich** auf **Symbole für die Anzeige auf der Taskleiste auswählen**.
  3. Aktivieren Sie den Schalter neben **Bitdefender-Agent**.

Wenn Sie dieses Icon doppelklicken wird sich Bitdefender öffnen. Wird das Symbol mit der rechten Maustaste angeklickt, öffnet sich ein Kontextmenü, mit dem Sie das BitdefenderProdukt verwalten können.



Tray Icon

- **Anzeigen** - Öffnet das Bitdefender-Hauptfenster.
- **Über** - Öffnet ein Fenster mit Informationen zu Bitdefender. Sie erfahren zudem, wo Sie bei unerwarteten Problemen Hilfe finden können und wo Sie die Abonnementvereinbarung sowie Informationen zu Komponenten von Drittanbietern und die Datenschutzrichtlinie aufrufen und nachlesen können.
- **Sicherheits-Widget anzeigen/ausblenden** - aktiviert/deaktiviert das Sicherheits-Widget.
- **Jetzt Aktualisieren** - startet ein sofortiges Update. Sie können den Update-Status im Update-Bereich des Bitdefender Hauptfensters verfolgen.

Das Bitdefender-Taskleistensymbol zeigt an, ob Probleme Ihr Gerät oder die Funktionsweise des Produkts beeinträchtigen. Dabei werden die folgende Symbole angezeigt:

Es gibt keine Probleme, die die Sicherheit Ihres Systems beeinträchtigen.

Kritische Probleme beeinträchtigen die Sicherheit Ihres Systems. Sie benötigen Ihre sofortige Aufmerksamkeit und müssen umgehend behoben werden.

Wenn Bitdefender nicht aktiv ist, ist das Symbol in der Task-Leiste grau hinterlegt: . Dies geschieht normalerweise, wenn das Abonnement abgelaufen ist. Es kann auch vorkommen, wenn die Bitdefender Services nicht reagieren oder andere Fehler die normale Funktionsweise von Bitdefender einschränken.

4.2. Navigationsmenü

Links in der Bitdefender-Benutzeroberfläche finden Sie das Navigationsmenü, über das Sie schnell und bequem auf die Bitdefender-Funktionen und -Tools zur Nutzung Ihres Produkts zugreifen können. In diesem Bereich finden Sie die folgenden Reiter:

- **Dashboard**. Von hier aus können Sie Sicherheitsprobleme schnell beheben, Empfehlungen anzeigen, die sich aus Ihren Systemanforderungen und Ihrem Nutzungsverhalten ableiten, sowie Schnellaktionen durchführen.
-
- **Schutz**. Von hier aus können Sie Virenschutz-Scans starten und konfigurieren, eventuell durch Ransomware verschlüsselte Daten wiederherstellen und den Schutz beim Surfen im Internet konfigurieren.

  Beachten Sie
  Some features are not available on the free version.

- **Benachrichtigungen**. Von hier aus können Sie Passwortmanager für Ihre Online-Konten erstellen, Online-Zahlungen in einer sicheren Umgebung vornehmen und die VPN-Anwendung öffnen.

  Beachten Sie
  Some features are not available on the free version.

- **Dienstprogramme**. Von hier aus können Sie Profile verwalten und auf die Datenschutzfunktion zugreifen.

Beachten Sie
Some features are not available on the free version.

- **Benachrichtigungen**. Von hier aus können Sie auf Ihre Benachrichtigungen zugreifen.
- **Einstellungen**. Von hier aus können Sie auf die allgemeinen Einstellungen zugreifen.

Oben im Hauptfenster finden Sie die Funktionen **Mein Konto** und **Support**.

- **Support**. Von hier aus können Sie jederzeit den technischen Support von Bitdefender kontaktieren, falls Sie Unterstützung mit Ihrem Bitdefender Antivirus Free benötigen.
- **Mein Konto**. Von hier aus können Sie Ihr Bitdefender-Benutzerkonto aufrufen, um Ihre Abonnements einzusehen und auf den von Ihnen verwalteten Geräten Sicherheitsaufgaben ausführen. Hier finden Sie auch Einzelheiten zu Ihrem Bitdefender-Benutzerkonto und dem aktuell verwendeten Abonnement.

4.3. Dashboard

Im [Dashboard-Fenster können Sie die häufigsten Aufgaben durchführen, Sicherheitsprobleme schnell und einfach beheben, Informationen über die Programmausführung anzeigen und auf die verschiedenen Bereiche zugreifen, über die sich die Produkteinstellungen konfigurieren lassen.

Und das alles mit nur wenigen Klicks.

Das Fenster ist in drei Hauptbereiche aufgeteilt:

Sicherheitsstatusbereich
: Hier können Sie den Sicherheitsstatus Ihres Geräts überprüfen.

Autopilot
: Hier können Sie die Empfehlungen des Autopilots einsehen, um eine einwandfreie Funktion des Systems zu gewährleisten.

Schnellaktionen
: Hier können Sie eine Reihe von Aufgaben durchführen, damit Ihr System geschützt bleibt.

Beachten Sie
Some tasks are not available on the free version.

4.3.1. Sicherheitsstatusbereich

Bitdefender nutzt ein System zur Problemverfolgung, um potenzielle Sicherheitsprobleme für Ihr Gerät und Ihre Daten zu erkennen und Sie darüber zu informieren. Zu den gefundenen Problemen gehören auch wichtige Schutzeinstellungen, die deaktiviert sind, und andere Umstände, die ein Sicherheitsrisiko darstellen.

Wenn Probleme die Sicherheit Ihres Geräts beeinträchtigen, wechselt die Farbe der Statusanzeige oben rechts in der Bitdefender-Benutzeroberfläche auf rot. Der angezeigte Status informiert Sie über die Art der Probleme, die Ihr System beeinträchtigen. Darüber hinaus wechselt das Symbol in der Taskleiste zu . Wenn Sie den Mauszeiger über das Symbol bewegen, bestätigt ein Pop-up-Fenster das Vorliegen ausstehender Probleme.

Da die erkannten Probleme verhindern könnten, dass Bitdefender Sie vor Bedrohungen schützt, bzw. auf ein ernstes Sicherheitsrisiko hinweisen könnten, empfehlen wir ein sofortiges Eingreifen und eine umgehende Behebung der Probleme. Klicken Sie auf die Schaltfläche neben dem erkannten Problem, um es zu beheben.

4.3.2. Autopilot

Um einen wirksamen Betrieb sicherzustellen und Ihnen besseren Schutz bei Ihren verschiedenen Aktivitäten zu bieten, dient der Bitdefender Autopilot als Ihr persönlicher Sicherheitsberater. Abhängig von Ihrer jeweiligen Aktivität, d. h. ob Sie arbeiten, Online-Zahlungen vornehmen, Filme anschauen oder Spiele spielen, liefert der Bitdefender Autopilot kontextabhängige Empfehlungen, die sich nach Ihrer Gerätenutzung und Ihren Anforderungen richten. Die vorgeschlagenen Empfehlungen können auch Maßnahmen umfassen, die Sie ergreifen sollten, um einen optimalen Betrieb Ihres Produkts sicherzustellen.

Klicken Sie auf die entsprechende Schaltfläche, um eine empfohlene Funktion zu nutzen oder Verbesserungen an Ihrem Produkt vorzunehmen.

Deaktivieren der Autopilot-Benachrichtigungen

Um Sie auf die Empfehlungen des Autopilots aufmerksam zu machen, zeigt Ihr Bitdefender-Produkt standardmäßig entsprechende Pop-up-Benachrichtigungen an.

So können Sie die Autopilot-Benachrichtigungen deaktivieren:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Einstellungen**.
2. Deaktivieren Sie im Fenster **Allgemein** die **Benachrichtigungen zu Empfehlungen**.

4.3.3. Schnellaktionen

Über die Schnellaktionen können Sie schnell und bequem Aufgaben starten, die Sie für den Schutz Ihres Systems und ein besseres Arbeiten als wichtig erachten.

Bitdefender umfasst standardmäßig eine Reihe von Schnellaktionen, die Sie jederzeit durch die von Ihnen am meisten genutzten Aktionen ersetzen können. So können Sie eine Schnellaktion ersetzen:

1. Klicken Sie auf das -Symbol oben rechts in der Karte, die Sie entfernen möchten.
2. Bewegen Sie den Mauszeiger auf die Karte, die Sie zum Hauptfenster hinzufügen möchten, und klicken Sie danach auf **HINZUFÜGEN**.

Sie können die folgenden Aufgaben zum Hauptfenster hinzufügen:

- **Quick-Scan**. Führen Sie einen Quick Scan durch, um umgehend potenzielle Bedrohungen zu identifizieren, die auf Ihrem Gerät vorliegen könnten.
- **System-Scan**. Führen Sie einen System-Scan durch, um sicherzustellen, dass Ihr Gerät frei von Bedrohungen ist.

To start protecting additional Windows devices:

1. Klicken Sie auf **Bitdefender auf einem weiteren Gerät installieren**.

   Ein neues Fenster wird angezeigt.
2. Klicken Sie auf **DOWNLOAD-LINK SENDEN**.
3. Follow the on-screen steps to install Bitdefender Antivirus Free on Windows-based devices.

4.4. Die Bitdefender-Bereiche

4.4. Die Bitdefender-Bereiche

Das Bitdefender-Produkt besteht aus drei in nützliche Funktionen unterteilten Bereichen, die Sie bei der Arbeit, beim Surfen im Internet und bei der Abwicklung von Online-Zahlungen schützen, Ihre Systemgeschwindigkeit deutlich steigern und viele weitere Vorteile bieten.

Um auf die Funktionen und bestimmte Bereiche zuzugreifen oder um Ihr Produkt zu konfigurieren, stehen in die folgenden Symbole im Navigationsbereich der Bitdefender-Benutzeroberfläche zur Verfügung:

-  Schutz
-  Privatsphäre
-  Dienstprogramme

4.4.1. Schutz

In the Protection section you can configure security settings or configure and run scan tasks.

Im Bereich Schutz können Sie die folgenden Funktionen verwalten:

ANTIVIRUS

Der Virenschutz bildet die Grundlage Ihrer Sicherheit. Bitdefender schützt Sie sowohl in Echtzeit als auch bei Bedarf vor allen Arten von Bedrohungen, so zum Beispiel vor Malware, Trojanern, Spyware, Adware usw.

Über die Funktion Virenschutz können Sie schnell und bequem auf die folgenden Scan-Aufgaben zugreifen:

- Quick-Scan
- System-Scan
- Scans verwalten

Weitere Informationen zu den Scan-Aufgaben und eine Anleitung, wie Sie den Virenschutz konfigurieren können, finden Sie im Kapitel *„Virenschutz“* (S. 60).

ONLINE-GEFAHRENABWEHR

Mit der Online-Gefahrenabwehr schützen Sie sich beim Surfen im Netz zuverlässig vor Phishing-Angriffen, Betrugsversuchen und der Offenlegung privater Daten.

Weitere Informationen, wie man Bitdefender zum Schutz Ihrer Internet-Aktivitäten konfigurieren kann, finden Sie im Kapitel *„Online-Gefahrenabwehr“* (S. 81).

ERWEITERTE GEFAHRENABWEHR

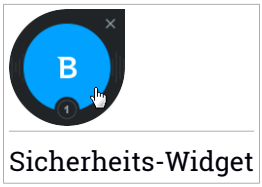
Die Erweiterte Gefahrenabwehr schützt Ihr System aktiv vor Bedrohungen wie Ransomware, Spyware und Trojanern, indem es das Verhalten aller installierten Anwendungen untersucht. Verdächtige Prozesse werden erkannt und, falls erforderlich, blockiert.

Weitere Informationen zum Schutz Ihres Systems vor Bedrohungen finden Sie im Kapitel *„Erweiterte Gefahrenabwehr“* (S. 78).

4.5. Sicherheits-Widget

Das **Sicherheits-Widget** ist die bequemste und schnellste Art Bitdefender Antivirus Free zu steuern. Wenn Sie dieses kleine, unauffällige Widget auf Ihren Desktop legen, haben Sie jederzeit wichtige Informationen im Blick und können zentrale Aufgaben ausführen:

- Öffnet das Bitdefender-Hauptfenster.
- Scan-Activität in Echtzeit überwachen;
- den Sicherheitsstatus Ihres Systems überwachen und gefundene Probleme beheben;
- Zeigt an, wenn ein Update durchgeführt wird.
- Benachrichtigungen und Ereignisprotokolle von Bitdefender lesen;
- Dateien und Ordner (einzeln oder als Gruppe) scannen, indem Sie sie auf das Widget ziehen;



Sicherheits-Widget

Der Gesamtsicherheitsstatus Ihres Computers wird **in der Mitte** des Widgets angezeigt. Farbe und Form des Symbols in der Mitte zeigen unterschiedliche Status an.

Ihr System ist derzeit gefährdet.

Sie benötigen Ihre sofortige Aufmerksamkeit und müssen umgehend behoben werden. Klicken Sie auf das Statussymbol, um die gemeldeten Probleme zu beheben.

Bitdefender-Dienste antworten nicht.

Ihr System ist geschützt.

Während eine Scan-Aufgabe ausgeführt wird, wird dieses animierte Symbol angezeigt.

Dieses Symbol zeigt an, dass Ihr Bitdefender-Abonnement abgelaufen ist.

Wenn ein Update ausgeführt wird, wird dieses Symbol angezeigt.

Wenn Probleme gemeldet werden, klicken Sie auf das Statussymbol, um den Problembehebungsassistenten zu starten.

Im unteren Bereich des Widgets werden die ungelesenen Ereignisse angezeigt (die Anzahl der unbeachteten Ereignisse, die Bitdefender gemeldet hat). Klicken Sie auf den Ereigniszähler, der z. B. bei einem ungelesenen Ereignis so 1 aussieht, um das Benachrichtigungsfenster zu öffnen. Weitere Informationen finden Sie im Kapitel ???.

4.5.1. Dateien und Verzeichnis scannen

Mit dem Sicherheits-Widget können Sie ganz einfach Dateien und Ordner scannen. Sie können Dateien und/oder Ordner einfach auf das **Sicherheits-Widget** ziehen und dort ablegen, um diese(n) Datei/Ordner zu scannen.

Der Viren-Scan-Assistent wird angezeigt. Er führt Sie durch den Scan-Vorgang. Die Scan-Optionen sind für bestmögliche Erkennungsraten vorkonfiguriert und können nicht verändert werden. Falls infizierte Dateien gefunden werden, wird Bitdefender versuchen, diese zu desinfizieren (den Schad-Code zu entfernen). Wenn die Desinfizierung fehlschlagen sollte, wird Ihnen der Viren-Scan-Assistent andere Möglichkeiten anbieten, wie mit den infizierten Dateien verfahren werden soll.

4.5.2. Das Sicherheits-Widget ausblenden/anzeigen

Wenn Sie das Widget nicht mehr angezeigt bekommen möchten, klicken Sie einfach auf ⊗.

Verwenden Sie eine der folgenden Methoden, um das Sicherheits-Widget wiederherzustellen:

- Über die Task-Leiste:
  1. Klicken Sie mit der rechten Maustaste auf das Bitdefender-Symbol in der Taskleiste.
  2. Klicken Sie im daraufhin angezeigten Kontextmenü auf **Sicherheits-Widget anzeigen**.
- Über die Bitdefender-Benutzeroberfläche:
  1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Einstellungen**.
  2. Aktivieren Sie im Fenster **Allgemein** das **Sicherheits-Widget**.

Das Bitdefender-Sicherheits-Widget ist standardmäßig deaktiviert.

4.6. Produktsprache ändern

Die Bitdefender-Benutzeroberfläche ist in mehreren Sprachen verfügbar. Gehen Sie zum Ändern der Sprache wie folgt vor:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Einstellungen**.
2. Klicken Sie im Fenster **Allgemein** auf **Sprache ändern**.
3. Wählen Sie die gewünschte Sprache aus der Liste aus und klicken Sie auf **SPEICHERN**.
4. Warten Sie einen Moment, bis die Einstellungen übernommen wurden.

5. BITDEFENDER CENTRAL

Bitdefender Central stellt Ihnen eine Plattform zur Verfügung, über die Sie auf die Online-Funktionen und -Dienste des Produkts zugreifen und wichtige Aufgaben auf allen Geräten ausführen können, auf denen Bitdefender installiert ist. Sie benötigen lediglich eine Internetverbindung, um sich mit jedem beliebigen Gerät bei Ihrem Bitdefender-Konto anzumelden. https://central.bitdefender.com Alternativ können Sie auf Android- und iOS-Geräten auch die Bitdefender Central-App nutzen.

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:

- Download and install Bitdefender on Windows based devices.
- Neue Geräte zu Ihrem Netzwerk hinzufügen und diese Geräte aus der Ferne verwalten.

5.1. So können Sie Bitdefender Central aufrufen:

Bitdefender Central kann auf verschiedene Weise aufgerufen werden:

- Über das Bitdefender-Hauptfenster:
  1. Klicken Sie auf das  -Symbol oben rechts in der Bitdefender-Oberfläche.
  2. Klicken Sie auf **Bitdefender Central aufrufen**.
  3. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Bitdefender-Konto an.
- 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 Bitdefender-Konto an.

- Auf Android- und iOS-Geräten:

  Öffnen Sie die bei Ihnen installierte Bitdefender Central-App.

Beachten Sie
Hier finden Sie alle Optionen und Anleitungen, die Ihnen über die Web-Plattform zur Verfügung gestellt werden.

5.2. 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.

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. Rufen Sie Bitdefender Central auf.
2. Klicken Sie auf das -Symbol in der rechten oberen Bildschirmecke.
3. Klicken Sie im Slide-Menü auf **Bitdefender-Konto**.
4. Wechseln Sie zum Reiter **Passwort und Sicherheit**.
5. Klicken Sie auf **Zwei-Faktor-Authentifizierung**.
6. Klicken Sie auf **ERSTE SCHRITTE**.

   Wählen Sie eine der folgenden Methoden aus:

- **Authentifizierungs-App** - Verwenden Sie eine Authentifizierungs-App, um für jede Anmeldung bei Ihrem Bitdefender-Konto einen Code zu generieren.

  Wenn Sie eine Authentifizierungs-App verwenden möchten, sich aber nicht sicher sind, welche App Sie verwenden sollen, können Sie sie aus einer Liste mit den von uns empfohlenen Authentifizierungs-Apps auswählen.

  a. Klicken 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 Desktop können Sie den angezeigten Code manuell eingeben.

     Klicken Sie auf **FORTFAHREN**.

  c. Geben Sie den von der App generierten bzw. den im vorherigen Schritt angezeigten Code ein, und klicken 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 geben Sie dann den erhaltenen Code ein.

  a. Klicken 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, Ihr E-Mail-Konto aufzurufen und den generierten Code einzugeben. ach Ablauf dieser Zeit müssen Sie einen neuen Code generieren, indem Sie die gleichen Schritte erneut ausführen.

  c. Klicken 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 darf nur einmal verwendet werden.

  e. Klicken Sie auf **FERTIG**.

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

1. Klicken 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. ach Ablauf dieser Zeit müssen Sie einen neuen Code generieren, indem Sie die gleichen Schritte erneut ausführen.
3. Bestätigen Sie Ihre Auswahl.

5.2.1. 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. Rufen Sie Bitdefender Central auf.
2. Klicken Sie auf das -Symbol in der rechten oberen Bildschirmecke.
3. Klicken Sie im Slide-Menü auf **Bitdefender-Konto**.
4. Wechseln Sie zum Reiter **Passwort und Sicherheit**.
5. Klicken Sie auf **Vertrauenswürdige Geräte**.
6. Es wird eine Liste mit Geräten angezeigt, auf denen Bitdefender installiert ist. Klicken 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.

5.3. Meine Abonnements

The Bitdefender Central platform gives you the possibility to easily see the subscriptions you have for all your devices.

5.3.1. Verfügbare Abonnements anzeigen

So können Sie Ihre verfügbaren Abonnements anzeigen:

1. Rufen Sie Bitdefender Central auf.

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.

Beachten Sie
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.

5.3.2. Ein neues Gerät hinzufügen

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

1. Rufen Sie Bitdefender Central auf.
2. Rufen Sie den Bereich **Meine Geräte** auf und klicken Sie auf das -Symbol.
3. Wählen Sie eine der beiden verfügbaren Optionen:
   - **Dieses Gerät schützen**

     Wählen Sie diese Option und danach den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, klicken Sie auf die entsprechende Schaltfläche.
   - **Andere Geräte schützen**

     Wählen Sie diese Option und danach den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, klicken 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.

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

4. Warten Sie, bis der Download abgeschlossen ist, und führen Sie das Installationsprogramm aus.

5.3.3. Abonnement aktivieren

A paid subscription can be activated during the installation process by using your Bitdefender account. Together with the activation process, its validity starts to count-down.

Falls Sie einen Aktivierungscode von einem unserer Wiederverkäufer gekauft oder diesen als Geschenk erhalten haben, können Sie die Gültigkeitsdauer eines bestehenden Bitdefender-Abonnements unter diesem Benutzerkonto um diesen Zeitraum verlängern, vorausgesetzt es handelt sich um einen Code für das gleiche Produkt.

So können Sie ein Abonnement mithilfe eines Aktivierungscodes aktivieren:

1. Rufen Sie Bitdefender Central auf.
2. Rufen Sie den Bereich **Meine Abonnements** auf.
3. Klicken Sie auf **+Mit Code aktivieren** und geben Sie den Code in das entsprechende Feld ein.
4. Klicken Sie zum Fortfahren auf **AKTIVIEREN**.

Das Abonnement wurde aktiviert. Rufen Sie den Bereich **Meine Geräte** auf und klicken Sie auf das -Symbol, um das Produkt auf einem Ihrer Geräte zu installieren.

Beachten Sie
If you activate a subscription with activation code, the existing free subscription will be replaced with the paid subsctiption.

5.4. Meine Geräte

Über Ihr Bitdefender Central können Sie im Bereich **Meine Geräte** die Bitdefender-Produkte auf Ihren Geräten verwalten, vorausgesetzt, diese sind eingeschaltet und mit dem Internet verbunden. Auf den Gerätekacheln sind der Gerätename, das Betriebssystem, die installierten Produkte, der Sicherheitsstatus angegeben sowie die Information, ob Sicherheitsprobleme auf Ihren Geräten bestehen.

Um eine nach Status oder Benutzer geordnete Liste mit allen Geräten anzuzeigen, klicken Sie oben rechts auf dem Bildschirm auf den Drop-down-Pfeil.

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

1. Rufen Sie Bitdefender Central auf.
2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie in der entsprechenden Gerätekachel auf **DETAILS ANZEIGEN** und dann auf das ⋮ -Symbol in der rechten oberen Bildschirmecke.
4. Tippen Sie auf **Einstellungen**.
5. Geben Sie einen neuen Namen in das Feld **Gerätename** ein und clicken Sie dann auf **SPEICHERN**.

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

1. Rufen Sie Bitdefender Central auf.
2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie in der entsprechenden Gerätekachel auf **DETAILS ANZEIGEN** und dann auf das ⋮ -Symbol in der rechten oberen Bildschirmecke.
4. Wählen Sie **Profil**.
5. Klicken Sie auf **Besitzer hinzufügen** und füllen Sie dann die entsprechenden Felder aus. Passen Sie das Profil nach Bedarf an, indem Sie ein Foto hinzufügen und einen Geburtstag eingeben.
6. Klicken Sie auf **HINZUFÜGEN**, um das Profil zu speichern.
7. Wählen Sie aus der **Gerätebesitzer**-Liste den gewünschten Besitzer aus und klicken Sie auf **ZUORDNEN**.

So können Sie Bitdefender per Fernzugriff auf einem Windows-Gerät aktualisieren:

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

3. Klicken Sie in der entsprechenden Gerätekachel auf **DETAILS ANZEIGEN** und dann auf das ⋮ -Symbol in der rechten oberen Bildschirmecke.
4. Wählen Sie **Update**.

Klicken Sie in der entsprechenden Gerätekachel auf **DETAILS ANZEIGEN**, um das Gerät per Fernzugriff zu steuern oder Informationen zu Ihrem Bitdefender-Produkt auf einem bestimmten Geräte anzuzeigen.

Mit einem Klick auf **DETAILS ANZEIGEN** in einer Gerätekachel werden die folgenden Reiter angezeigt:

- **Dashboard**. In this window you can view details about the selected device, check its protection status and how many threats have been blocked in the last seven days. The protection status can be green, when there is no issue affecting your device, yellow when the device needs your attention or red when the device is at risk. When there are issues affecting your device, click the drop-down arrow in the upper status area to find out more details. From here you can manually fix issues that are affecting the security of your devices.
- **Schutz**. Über dieses Fenster können Sie per Fernzugriff einen Quick Scan oder eine Systemprüfung veranlassen. Klicken Sie auf **SCAN**, um den Vorgang zu starten. Sie können auch nachvollziehen, wann der letzte Scan auf dem Gerät durchgeführt wurde, und einen Bericht für den aktuellsten Scan abrufen, in dem die wichtigsten Informationen zusammengefasst werden.Weitere Informationen zu diesen Scan-Optionen finden Sie in den Kapiteln Abschnitt 11.2.3, „*Durchführen von System-Scans*“ und „*Durchführen von Quick Scans*“ (S. 62).

5.5. 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 deren Schutzstatus einsehen. Um Probleme auf den erkannten Geräten per Fernzugriff zu beheben, klicken Sie auf **Probleme beheben** und dann auf **SCANEN 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.

- **Blockierte Bedrohungen**. 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.

5.6. 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.

6. BITDEFENDER AUF DEM NEUESTEN STAND HALTEN

Jeden Tag werden neue Bedrohungen entdeckt und identifiziert. Darum ist so wichtig, dass Bitdefender jederzeit über die neuesten Bedrohungsinformationen verfügt.

Falls Sie über eine Breitbandverbindung oder eine DSL-Verbindung verfügen, arbeitet Bitdefender eigenständig. Die Software such standardmäßig nach Updates, wenn Sie Ihr Gerät einschalten und danach einmal pro **Stunde**. Wenn ein neues Update gefunden wird, wird es automatisch auf Ihr Gerät heruntergeladen und installiert.

Der Updatevorgang wird "on the fly" durchgeführt. Das bedeutet, dass die entsprechenden Dateien stufenweise aktualisiert werden. So stört der Updatevorgang nicht den Betrieb des Produkts, während gleichzeitig alle Schwachstellen behoben werden.

Wichtig
Um immer vor den neuesten Bedrohungen geschützt zu sein, sollte das automatische Update immer aktiviert bleiben.

In manchen Situationen kann es notwendig werden, dass Sie eingreifen, um den Bitdefender-Schutz auf dem neuesten Stand zu halten:

- Wenn Ihr Gerät über einen Proxy-Server mit dem Internet verbunden ist, müssen Sie die Proxy-Einstellungen wie unter *„Wie konfiguriere ich Bitdefender für die Nutzung einer Proxy-Verbindung?“* (S. 53) beschrieben konfigurieren.
- Falls Sie sich per Einwahl mit dem Internet verbinden, ist es sinnvoll, regelmäßig ein manuelles Bitdefender-Update durchzuführen. Weitere Informationen finden Sie im Kapitel *„Durchführung eines Updates“* (S. 33).

6.1. Überprüfen, ob Bitdefender auf dem neuesten Stand ist

So können Sie den Zeitpunkt des letzten Bitdefender-Updates erfahren:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Benachrichtigungen**.

2. Wählen Sie unter dem Reiter **Alle** die Benachrichtigung bezüglich des neuesten Updates aus.

Sie können herausfinden, wann Updates angestoßen wurden und weitere Informationen dazu einholen (d.h. ob sie erfolgreich waren oder nicht, ob ein Neustart erforderlich ist, um die Installation abzuschließen). Falls nötig starten Sie das System sobald es Ihnen möglich ist neu.

6.2. Durchführung eines Updates

Sie benötigen eine Internet-Verbindung, um Updates durchzuführen.

Rechtsklicken Sie zum Start eines Updates in der Taskleiste auf das Bitdefender-Symbol und wählen Sie **Jetzt aktualisieren**.

Die Funktion Update stellt eine Verbindung mit dem Bitdefender-Update-Server her und sucht nach verfügbaren Updates. Wenn ein Update erkannt wird, werden Sie abhängig von den Update-Einstellungen entweder aufgefordert, dies zu bestätigen oder das Update wird automatisch durchgeführt.

Wichtig
Es kann erforderlich sein, das Gerät nach Abschluss des Updates neu zu starten. Wir empfehlen, das so bald wie möglich zu tun.

Sie können die Updates auf Ihren Geräten zudem per Fernzugriff vornehmen, vorausgesetzt, sie sind eingeschaltet und mit dem Internet verbunden.

So können Sie Bitdefender per Fernzugriff auf einem Windows-Gerät aktualisieren:

1. Rufen Sie Bitdefender Central auf.
2. Rufen Sie den Bereich **Meine Geräte** auf.
3. Klicken Sie in der entsprechenden Gerätekachel auf **DETAILS ANZEIGEN** und dann auf das -Symbol in der rechten oberen Bildschirmecke.
4. Wählen Sie **Update**.

6.3. Aktivieren / Deaktivieren der automatischen Updates

So können Sie automatische Updates aktivieren oder deaktivieren:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Einstellungen**.
2. Wechseln Sie zum Reiter **Update**.
3. Aktivieren oder deaktivieren Sie den entsprechenden Schalter.
4. Ein Warnung wird angezeigt. Sie müssen Ihre Auswahl bestätigen, indem Sie im Menü wählen, wie lange die automatischen Updates deaktiviert bleiben sollen. Sie können automatische Updates für 5, 15 oder 30 Minuten, 1 Stunde oder bis zum Neustart des Systems deaktivieren.

Warnung
Hierbei handelt es sich um ein grobes Sicherheitsrisiko. Wir empfehlen, die automatischen Updates so kurz wie möglich zu deaktivieren. Denn Bitdefender kann Sie nur dann gegen die neusten Bedrohungen schützen, wenn es auf dem neuesten Stand ist.

6.4. Update-Einstellungen anpassen

Updates können im lokalen Netzwerk, über das Internet, direkt oder durch einen Proxy-Server durchgeführt werden. Standardmäßig scannt Bitdefender jede Stunde auf neue Updates und installiert diese ohne Ihr Zutun.

Die standardmäßigen Update-Einstellungen eignen sich für die meisten Benutzer und es ist normalerweise nicht erforderlich, diese zu ändern.

So können Sie die Update-Einstellungen anpassen:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Einstellungen**.
2. Wechseln Sie zum Reiter **Update** und passen Sie die Einstellungen nach Ihren Wünschen an.

Update-Häufigkeit

Bitdefender ist für eine stündliche Update-Prüfung konfiguriert. Die Update-Häufigkeit lässt sich durch Schieben des entsprechenden Reglers auf den gewünschten Update-Zeitraum festlegen.

Update-Verarbeitungsregeln

Sobald ein Update verfügbar ist, lädt Bitdefender es automatisch herunter und installiert es, ohne Sie vorher zu benachrichtigen. Deaktivieren Sie die

Option **Update im Hintergrund**, wenn Sie über die Verfügbarkeit neuer Updates benachrichtigt werden möchten.

Manche Updates erfordern einen Neustart, um die Installation abzuschließen.

Sollte ein Update einen Neustart erforderlich machen, arbeitet Bitdefender standardmäßig mit den alten Dateien weiter, bis der Benutzer das Gerät aus eigenen Stücken neu startet. Dadurch soll verhindert werden, dass der Update-Prozess von Bitdefender den Benutzer in seiner Arbeit behindert.

Wenn Sie nach einem Update über die Notwendigkeit eines Neustarts informiert werden möchten, aktivieren Sie die **Neustartbenachrichtigung**.

6.5. Regelmäßige Updates

Um sicherzustellen, dass Sie immer mit der neuesten Version arbeiten, sucht Ihr Bitdefender automatisch nach Produktupdates. Diese Updates können neue Funktionen und Verbesserungen beinhalten, Produktprobleme beheben und automatische Upgrades auf eine neue Version umfassen. Wird eine neue Bitdefender-Version per Update ausgeliefert, werden benutzerdefinierte Einstellungen gespeichert und der Vorgang der De- und Neuinstallation wird übersprungen.

Diese Updates erfordern einen Neustart des Systems, um die Installation neuer Dateien zu initiieren. Ein Pop-up-Fenster fordert Sie auf das System neu zu starten, sobald das Update abgeschlossen wurde. Sollten Sie diese Benachrichtigung verpasst haben, können Sie im Fenster Benachrichtigungen beim Eintrag über das neueste Update auf **JETZT NEU STARTEN** klicken oder das System manuell neu starten.

GEWUSST WIE

7. INSTALLATION

7.1. Wie kann ich Bitdefender auf einem zweiten Gerät installieren?

If the subscription covers more than one device, you can use your Bitdefender account to activate a second PC.

So können Sie Bitdefender auf einem zweiten Gerät installieren:

1. Klinken Sie unten links in der Bitdefender-Oberfläche auf **Bitdefender auf einem weiteren Gerät installieren**.

   Ein neues Fenster wird angezeigt.

2. Klicken Sie auf **DOWNLOAD-LINK SENDEN**.
3. Folgen Sie den angezeigten Anleitung, um Bitdefender zu installieren.

Das neue Gerät, auf dem Sie das Bitdefender-Produkt installiert haben, wird ab sofort im Bitdefender Central-Dashboard angezeigt.

7.2. Wie kann ich Bitdefender neu installieren?

Die Folgenden sind typische Situationen, in denen Sie Bitdefender erneut installieren müssen:

- Sie haben das Betriebssystem neu installiert..
- Sie möchten Probleme beheben, die das System verlangsamt oder zum Absturz gebracht haben könnten.
- Ihr Bitdefender-Produkt startet nicht oder funktioniert nicht ordnungsgemäß.

Falls eine der genannten Situationen auf Sie zutrifft, gehen Sie bitte folgendermaßen vor:

- In **Windows 7**:
  1. Klicken Sie auf **Start** und **Alle Programme**.
  2. Suchen Sie **Bitdefender Antivirus Free** und wählen Sie **Deinstallieren**.
  3. Klicken Sie im angezeigten Fenster auf **NEU INSTALLIEREN**.
  4. Sie müssen das Gerät neu starten, um den Vorgang abzuschließen.

- In **Windows 8 und Windows 8.1**:
  1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
  2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
  3. Suchen Sie **Bitdefender Antivirus Free** und wählen Sie **Deinstallieren**.
  4. Klicken Sie im angezeigten Fenster auf **NEU INSTALLIEREN**.
  5. Sie müssen das Gerät neu starten, um den Vorgang abzuschließen.
- In **Windows 10**:
  1. Klicken Sie auf **Start** und danach auf Einstellungen.
  2. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie **Apps & Funktionen** aus.
  3. Suchen Sie **Bitdefender Antivirus Free** und wählen Sie **Deinstallieren**.
  4. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.
  5. Klicken Sie auf **NEU INSTALLIEREN**.
  6. Sie müssen das Gerät neu starten, um den Vorgang abzuschließen.

Beachten Sie
Wenn Sie bei der Neuinstallation wie hier beschrieben vorgehen, werden Ihre benutzerdefinierte Einstellungen gespeichert und sind im neu installierten Produkt wieder verfügbar. Weitere Einstellungen werden unter Umständen wieder auf die Standardkonfiguration zurückgesetzt.

7.3. Where can I download Bitdefender Antivirus Free from?

You can download Bitdefender Antivirus Free form the Bitdefender Website. Once the installation process is complete, Bitdefender Antivirus Free is activated.

Beachten Sie
Bevor Sie das Installationspaket ausführen, sollten Sie jede andere auf Ihrem System installierte Sicherheitslösung entfernen. Wenn Sie mehr als eine Sicherheitslösung auf Ihrem Gerät verwenden, wird dadurch das System instabil.

To download Bitdefender Antivirus Free from Bitdefender Website::

1. Access https://www.bitdefender.com/toolbox/.
2. Click download on Bitdefender Antivirus Free.
3. Warten Sie, bis der Download abgeschlossen ist, und führen Sie das Installationsprogramm aus.
4. Führen Sie das von Ihnen heruntergeladene Bitdefender aus.

7.4. Wie kann ich die Sprache für mein Bitdefender ändern?

Die Bitdefender-Benutzeroberfläche ist in mehreren Sprachen verfügbar. Gehen Sie zum Ändern der Sprache wie folgt vor:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Einstellungen**.
2. Klicken Sie im Fenster **Allgemein** auf **Sprache ändern**.
3. Wählen Sie die gewünschte Sprache aus der Liste aus und klicken Sie auf **SPEICHERN**.
4. Warten Sie einen Moment, bis die Einstellungen übernommen wurden.

8. BITDEFENDER CENTRAL

8.1. Wie melde ich mich mit einem anderen Konto bei Bitdefender an?

Sie haben ein neues Bitdefender-Konto angelegt und möchten es von nun an nutzen.

So melden Sie sich mit einem anderen Bitdefender-Konto an:

1. Klicken Sie oben im Bitdefender-Fenster auf Ihren Kontonamen.
2. Klicken Sie oben rechts im Bildschirm auf **Konto wechseln**, um das Gerät mit einem anderen Benutzerkonto zu verknüpfen.
3. Geben Sie die E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **WEITER**.
4. Geben Sie Ihr Passwort ein und klicken Sie auf **ANMELDEN**.

> **Beachten Sie**
> Das Bitdefender-Produkt auf Ihrem Gerät wird entsprechend dem mit Ihrem neuen Bitdefender-Konto verknüpften Abonnement automatisch umgestellt. Falls mit dem neuen Bitdefender-Konto kein verfügbares Abonnement verknüpft ist oder Sie es von einem früheren Benutzerkonto übernehmen möchten, können Sie sich wie in Kapitel *„Hilfe anfordern“* (S. 106) beschrieben mit dem Bitdefender-Support in Verbindung setzen.

8.2. Wie kann ich die Bitdefender Central-Hilfemeldungen deaktivieren?

Die Hilfemeldungen werden im Dashboard angezeigt, um Ihnen zu zeigen, wie Sie die verschiedenen Optionen in Bitdefender Central nutzen können.

So können Sie diese Meldungen deaktivieren:

1. Rufen Sie Bitdefender Central auf.
2. Klicken Sie auf das -Symbol in der rechten oberen Bildschirmecke.
3. Klicken Sie im Menü auf **Mein Konto**.
4. Klicken Sie im Slide-Menü auf **Einstellungen**.
5. Deaktivieren Sie die Option **Hilfemeldungen aktivieren/deaktivieren**.

8.3. Ich habe das Passwort vergessen, das ich für mein Bitdefender-Konto festgelegt habe. Wie kann ich es zurücksetzen?

Das Passwort für Ihr Bitdefender-Konto können Sie auf eine von zwei Arten ändern:

- Über die Bitdefender-Benutzeroberfläche:
  1. Klicken Sie auf das  -Symbol oben rechts in der Bitdefender-Oberfläche.
  2. Klicken Sie oben rechts im Bildschirm auf **Konto wechseln**.

     Ein neues Fenster wird angezeigt.
  3. Geben Sie Ihre E-Mail-Adresse ein und klicken Sie auf **WEITER**.

     Ein neues Fenster wird angezeigt.
  4. Klicken Sie auf **Passwort vergessen?**.
  5. Klicken Sie auf **WEITER**.
  6. Rufen Sie Ihre E-Mails ab, geben Sie den Sicherheitscode ein, den Sie per E-Mail bekommen haben, und klicken Sie auf **WEITER**.

     Oder Sie klicken in der E-Mail, die Sie von uns bekommen haben, auf **Passwort ändern**.
  7. Geben Sie Ihre gewünschtes neues Passwort ein. Geben Sie es dann noch ein zweites Mal ein. Klicken Sie auf **SPEICHERN**.
- Über Ihren Web-Browser:
  1. Gehen Sie zu: https://central.bitdefender.com.
  2. Klicken Sie auf **ANMELDEN**.
  3. Geben Sie Ihre E-Mail-Adresse ein und klicken Sie auf **WEITER**.
  4. Klicken Sie auf **Passwort vergessen?**.
  5. Klicken Sie auf **WEITER**.
  6. Rufen Sie Ihre E-Mails ab und folgen Sie der Anleitung, um ein neues Passwort für Ihr Bitdefender-Konto festzulegen.

Geben Sie von jetzt an Ihre E-Mail-Adresse und das neue Passwort ein, um auf Ihr Bitdefender-Konto zuzugreifen.

8.4. Wie kann ich die Benutzersitzungen in meinem Bitdefender-Konto verwalten?

In Ihrem Bitdefender-Konto können Sie die jüngsten inaktiven und aktiven Benutzersitzungen auf mit Ihrem Konto verbundenen Geräten verwalten. Außerdem können Sie sich aus der Ferne folgendermaßen abmelden:

1. Rufen Sie Bitdefender Central auf.
2. Klicken Sie auf das -Symbol in der rechten oberen Bildschirmecke.
3. Klicken Sie im Slide-Menü auf **Sitzungen**.
4. Wählen Sie im Bereich **Aktive Sitzungen** die Option **ABMELDEN** neben dem Gerät, für das Sie die Benutzersitzung beenden möchten.

9. PRÜFEN MIT BITDEFENDER

9.1. Wie kann ich eine Datei oder einen Ordner scannen?

Um eine Datei oder einen Ordner einfach und schnell zu scannen, klicken Sie mit der rechten Maustaste auf das Objekt, das Sie scannen möchten, wählen Sie Bitdefender und anschließend **Mit Bitdefender scannen** aus dem Menü.

Um den Scan abzuschließen, folgen Sie den Anweisungen des Scan-Assistenten. Bitdefender wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen.

Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

Typische Situationen, für die diese Scan-Methode geeignet ist:

- Sie vermuten, dass eine bestimmte Datei oder ein Ordner infiziert ist.
- Immer dann, wenn Sie aus dem Internet Dateien herunterladen, von deren Ungefährlichkeit Sie nicht überzeugt sind.
- Scannen Sie einen freigegebenen Ordner, bevor Sie die enthaltenen Dateien auf Ihr Gerät kopieren.

9.2. Wie scanne ich mein System?

So können Sie einen vollständigen System-Scan durchführen:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Öffnen**.
3. Klicken Sie neben **System-Scan** auf **Scan starten**.
4. Folgen Sie den Anweisungen des Scan-Assistenten, um den Scan abzuschließen. Bitdefender wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen.

   Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen. Weitere Informationen finden Sie im Kapitel *„Viren-Scan-Assistent“* (S. 67).

9.3. Wie plane ich einen Scan?

Sie können Ihr Bitdefender-Produkt so konfigurieren, dass es wichtige Systembereiche nur dann scannt, wenn Sie Ihr Gerät nicht benötigen.

So können Sie einen Scan planen:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Öffnen**.
3. Klicken Sie unten in der Benutzeroberfläche auf ••• neben dem Scan-Typ, den Sie planen möchten, System-Scan oder Quick Scan, und wählen Sie dann **Bearbeiten**.

   Alternativ können Sie einen individuellen Scan-Typ, indem Sie neben **Scans verwalten** auf **+Scan erstellen** klicken.
4. Richten Sie den Scan entsprechend Ihrer Anforderungen ein und klicken Sie auf **Weiter**.
5. Markieren Sie das Kästchen neben **Legen Sie fest, für wann Sie diese Aufgabe planen möchten**.

   Wählen Sie eine der entsprechenden Optionen, um einen Zeitplan festzulegen:

   - Beim Systemstart
   - Täglich
   - Wöchentlich
   - Monatlich

   Wenn Sie Täglich, Monatlich oder Wöchentlich wählen, ziehen Sie den Regler entlang der Skala, um den gewünschten Zeitraum festzulegen, in dem der geplante Scan beginnen soll.

Wenn Sie einen neuen benutzerdefinierten Scan erstellen möchten, erscheint das Fenster **Scan-Aufgabe**. Hier können Sie die Systembereiche auswählen, die gescannt werden sollen.

9.4. Wie kann ich eine benutzerdefinierte Scan-Aufgabe anlegen?

Wenn Sie bestimmte Bereiche Ihres Geräts scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierte Scan-Aufgabe konfigurieren und ausführen.

Um eine benutzerdefinierte Scan-Aufgabe anzulegen, gehen Sie folgendermaßen vor:

1. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Öffnen**.
2. Klicken Sie neben **+Scan erstellen** auf **Scans verwalten**.
3. Geben Sie im Namensfeld einen Namen für den Scan ein, wählen Sie die Bereiche aus, die Sie scannen möchten, und klicken Sie auf **WEITER**.
4. Konfigurieren Sie diese allgemeinen Optionen:
   - **Nur Anwendungen scannen**. Sie können Bitdefender so konfigurieren, dass nur aufgerufene Apps gescannt werden.
   - **Priorität der Scan-Aufgabe**. Sie können festlegen, wie sich ein Scan-Vorgang auf die Systemleistung auswirkt.
     - Auto - Die Priorität des Scan-Vorgangs hängt von der Systemaktivität ab. Um sicherzustellen, dass der Scan-Vorgang die Systemaktivität nicht beeinträchtigt, entscheidet Bitdefender, ob der Scan-Vorgang mit hoher oder niedriger Priorität ausgeführt wird.
     - Hoch - Die Priorität des Scan-Vorgangs wird als hoch festgelegt. Wenn Sie diese Option wählen, können andere Programme langsamer ausgeführt werden. So kann der Scan-Vorgang schneller abgeschlossen werden.
     - Niedrig - Die Priorität des Scan-Vorgangs wird als niedrig festgelegt. Wenn Sie diese Option wählen, können andere Programme schneller ausgeführt werden. So dauert es länger, bis der Scan-Vorgang abgeschlossen wird.
   - **Aktionen nach dem Scan**. Wählen Sie die Aktion, die von Bitdefender durchgeführt werden soll, wenn keine Bedrohungen gefunden wurden:
     - Übersichtsfenster anzeigen
     - Gerät herunterfahren

- Scan-Fenster schließen

5. Um die Scan-Optionen im Detail zu konfigurieren, klicken Sie auf **Erweiterte Optionen anzeigen**.

   Klicken Sie auf **Weiter**.

6. Sie können bei Bedarf die Option **Scan-Aufgabe planen** aktivieren und dann festlegen, wann der von Ihnen erstellte benutzerdefinierte Scan gestartet werden soll.

   - Beim Systemstart
   - Täglich
   - Monatlich
   - Wöchentlich

   Wenn Sie Täglich, Monatlich oder Wöchentlich wählen, ziehen Sie den Regler entlang der Skala, um den gewünschten Zeitraum festzulegen, in dem der geplante Scan beginnen soll.

7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Konfigurationsfenster zu schließen.

   Abhängig von den Bereichen, die gescannt werden sollen, kann der Scan einige Zeit in Anspruch nehmen. Wenn während des Scan-Vorgangs Bedrohungen gefunden werden, werden Sie aufgefordert, die Aktionen auszuwählen, die für die erkannten Dateien durchgeführt werden sollen.

Bei Bedarf können Sie einen bereits durchgeführten benutzerdefinierten Scan einfach erneut ausführen, indem Sie auf den entsprechenden Eintrag in der Liste klicken.

9.5. Wie kann ich einen Ordner vom Scan ausnehmen?

Mit Bitdefender können Sie bestimmte Dateien, Ordner oder Dateiendungen vom Scan ausnehmen.

Ausnahmen sollten nur von Benutzern genutzt werden, die erfahren im Umgang mit Computern sind und nur in den folgenden Situationen:

- Sie haben einen großen Ordner mit Filmen und Musik auf Ihrem System gespeichert.
- Sie haben ein großes Archiv mit verschiedenen Daten auf Ihrem System gespeichert.

- Sie haben einen Ordner, in dem Sie verschiedene Software-Typen und Anwendungen zu Testzwecken installieren. Ein Scan des Ordners könnte zum Verlust einiger der Daten führen.

So können Sie einen Ordner Ausschlussliste hinzufügen:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Öffnen**.
3. Klicken Sie auf den Tab **Einstellungen**.
4. Klicken Sie auf **Ausnahmen verwalten**.
5. Klicken Sie auf **+Ausnahme hinzufügen**.
6. Geben Sie den Pfad des Ordners, den Sie vom Scan ausnehmen möchten, in das entsprechende Feld ein.

   Alternativ können Sie zu dem Ordner navigieren, indem Sie rechts in der Benutzeroberfläche auf die Schaltfläche "Durchsuchen" klicken, ihn auswählen und dann auf **OK** klicken.
7. Aktivieren Sie den Schalter neben der Schutzfunktion, durch die der Ordner nicht gescannt werden soll. Sie haben drei Optionen:
   - Virenschutz
   - Online-Gefahrenabwehr
   - Erweiterte Gefahrenabwehr
8. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Fenster zu schließen.

9.6. Wie gehe ich vor, wenn Bitdefender eine saubere Datei als infiziert eingestuft hat?

Es können Situationen auftreten, in denen Bitdefender einwandfreie Dateien irrtümlicherweise als Bedrohung einstuft (Fehlalarm). Um diesen Fehler zu korrigieren, fügen Sie die Datei der Bitdefender-Ausnahmeliste hinzu:

1. Deaktivieren Sie den Bitdefender-Echtzeitvirenschutz:
   a. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
   b. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Öffnen**.

c. Deaktivieren Sie im Fenster **Erweitert** die Option **Bitdefender-Schild**.

Ein Warnung wird angezeigt. Sie müssen Ihre Auswahl bestätigen, indem Sie im Menü wählen, wie lange der Echtzeitschutz deaktiviert bleiben soll. Sie können den Echtzeitschutz für 5, 15 oder 30 Minuten, 1 Stunde, dauerhaft oder bis zum Neustart des Systems deaktivieren.

2. Lassen Sie sich die verborgenen Objekte in Windows anzeigen. Eine Anleitung hierzu finden Sie im Kapitel *„Wie kann ich in Windows versteckte Objekte anzeigen?“* (S. 55).
3. Stellen Sie die Datei aus der Quarantäne wieder her:
   a. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
   b. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Öffnen**.
   c. Rufen Sie das Fenster **Einstellungen** auf und klicken Sie auf **Quarantäne verwalten**.
   d. Wählen Sie die Datei aus und klicken Sie auf **Wiederherstellen**.
4. Fügen Sie die Datei zur Ausnahmeliste hinzu. Eine Anleitung hierzu finden Sie im Kapitel *„Wie kann ich einen Ordner vom Scan ausnehmen?“* (S. 46).

   Standardmäßig fügt Bitdefender wiederhergestellte Dateien automatisch zur Ausnahmeliste hinzu.
5. Aktivieren Sie den Bitdefender-Echtzeitvirenschutz.
6. Setzten Sie sich mit unseren Support-Mitarbeitern in Verbindung, damit wir die Erkennung des Updates der Bedrohungsinformationen entfernen können. Eine Anleitung hierzu finden Sie im Kapitel *„Hilfe anfordern“* (S. 106).

9.7. Wo sehe ich, welche Bedrohungen Bitdefender gefunden hat?

Nach jedem durchgeführten Scan wird ein Protokoll erstellt, in dem Bitdefender alle gefundenen Probleme aufzeichnet.

Der Bericht enthält detaillierte Informationen über den Scan-Vorgang, so wie Scan-Optionen, das Scan-Ziel, die gefundenen Bedrohungen und die Aktionen, die für diese Bedrohungen ausgeführt wurden.

Sobald der Scan beendet ist, können Sie das Scan-Protokoll direkt aus dem Scan-Assistenten heraus öffnen, indem Sie auf **PROTOKOLL ANZEIGEN** klicken.

So können Sie ein Scan-Protokoll oder gefundene Infektionen auch später anzeigen:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Benachrichtigungen**.
2. Wählen Sie unter dem Reiter **Alle** die Benachrichtigung bezüglich des neuesten Scans aus.

   Hier können Sie alle Ereignisse des Bedrohungs-Scans finden, einschließlich der Bedrohungen, die während Zugriff-Scans und vom Benutzer gestarteten Scans entdeckt wurden. Dazu kommen Statusänderungen für automatische Scans.
3. In der Benachrichtigungsliste können Sie überprüfen, welche Scans kürzlich durchgeführt wurden. Klicken Sie auf eine Benachrichtigung, um mehr darüber zu erfahren.
4. Um ein Scan-Protokoll zu öffnen, klicken Sie auf **Protokoll anzeigen**.

10. NÜTZLICHE INFORMATIONEN

10.1. Wie kann ich meine Sicherheitslösung selbst testen?

Um die ordnungsgemäße Funktion Ihres Bitdefender-Produkts zu überprüfen, empfehlen wir den EICAR-Test.

Dabei testen Sie mithilfe der speziell für diesen Zweck entwickelten EICAR-Testdatei Ihre Sicherheitslösung.

Gehen Sie folgendermaßen vor, um Ihre Sicherheitslösung zu testen:

1. Laden Sie die Testdatei von der offiziellen EICAR-Website unter http://www.eicar.org/ herunter.
2. Wechseln Sie zum Reiter **Anti-Malware Testfile**.
3. Klicken Sie im Menü links auf **Download**.
4. Klicken Sie unter **Download area using the standard protocol http** auf die **eicar.com**-Testdatei.
5. Sie werden informiert, dass die von Ihnen aufgerufene Seite die EICAR-Testdatei (keine Bedrohung) enthält.

   Wenn Sie auf **Ich bin mir der Risiken bewusst und möchte trotzdem fortfahren** klicken, beginnt der Download der Testdatei und ein Bitdefender-Fenster informiert Sie, dass eine Bedrohung erkannt wurde.

   Klicken Sie auf **Mehr...** für weitere Informationen.

Falls Sie keine Bitdefender-Benachrichtigung erhalten, empfehlen wir Ihnen, sich wie in Kapitel *„Hilfe anfordern“ (S. 106)* beschrieben an Bitdefender zu wenden.

10.2. Wie kann ich Bitdefender entfernen?

So können Sie Ihr Bitdefender Antivirus Free entfernen:

- In **Windows 7**:
  1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
  2. Suchen Sie **Bitdefender Antivirus Free** und wählen Sie **Deinstallieren**.

3. Klicken Sie im angezeigten Fenster auf **Entfernen**.
4. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.

- In **Windows 8 und Windows 8.1**:
  1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
  2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
  3. Suchen Sie **Bitdefender Antivirus Free** und wählen Sie **Deinstallieren**.
  4. Klicken Sie im angezeigten Fenster auf **Entfernen**.
  5. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.
- In **Windows 10**:
  1. Klicken Sie auf **Start** und danach auf Einstellungen.
  2. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und danach auf **Apps**.
  3. Suchen Sie **Bitdefender Antivirus Free** und wählen Sie **Deinstallieren**.
  4. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.
  5. Klicken Sie im angezeigten Fenster auf **Entfernen**.
  6. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.

Beachten Sie
Wenn Sie bei der Neuinstallation so vorgehen, werden die benutzerdefinierten Einstellungen endgültig gelöscht.

10.3. Wie fahre ich das Gerät automatisch herunter, nachdem der Scan beendet wurde?

Bitdefender bietet unterschiedliche Scan-Aufgaben, mithilfe derer Sie sicherstellen können, dass Ihr System nicht durch Bedrohungen infiziert wurde. Je nach Software- und Hardwarekonfiguration kann ein Scan des gesamten Systems längere Zeit in Anspruch nehmen.

Deshalb können Sie Bitdefender so konfigurieren, dass Ihr Produkt den Computer herunterfährt, sobald der Scan abgeschlossen ist.

Stellen Sie sich folgende Situation vor: Sie sind mit der Arbeit fertig und möchten ins Bett gehen. Sie möchten aber nun noch Ihr System durch Bitdefender auf Bedrohungen prüfen lassen.

Gehen Sie folgt vor, um das Gerät herunterzufahren, sobald ein Quick-Scan oder System-Scan beendet wurde:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Öffnen**.
3. Klicken Sie im Fenster **Scans** neben Quick Scan oder System-Scan auf ••• und wählen Sie **Bearbeiten**.
4. Richten Sie den Scan entsprechend Ihrer Anforderungen ein und klicken Sie auf **Weiter**.
5. Markieren Sie das Kästchen neben **Legen Sie fest, für wann Sie diese Aufgabe planen möchten**, und legen Sie fest, wann die Aufgabe beginnen soll.

   Wenn Sie Täglich, Monatlich oder Wöchentlich wählen, ziehen Sie den Regler entlang der Skala, um den gewünschten Zeitraum festzulegen, in dem der geplante Scan beginnen soll.
6. Klicken Sie auf **Speichern**.

Gehen Sie wie folgt vor, um das Gerät nach Abschluss eines benutzerdefinierten Scans herunterzufahren:

1. Klicken Sie neben dem von Ihnen erstellten benutzerdefinierten Scan auf •••.
2. Klicken Sie auf **Weiter** und dann erneut auf **Weiter**.
3. Markieren Sie das Kästchen neben **Legen Sie fest, für wann Sie diese Aufgabe planen möchten**, und legen Sie fest, wann die Aufgabe beginnen soll.
4. Klicken Sie auf **Speichern**.

Wenn keine Bedrohungen gefunden wurden, wird das Gerät heruntergefahren.

Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen. Weitere Informationen finden Sie im Kapitel *„Viren-Scan-Assistent“ (S. 67)*.

10.4. Wie konfiguriere ich Bitdefender für die Nutzung einer Proxy-Verbindung?

Wenn sich Ihr Gerät über einen Proxy-Server mit dem Internet verbindet, müssen Sie Bitdefender mit den Proxy-Einstellungen konfigurieren. Normalerweise findet und importiert Bitdefender automatisch die Proxy-Einstellungen Ihres Systems.

Wichtig
Internet-Verbindungen in Privathaushalten nutzen üblicherweise keine Proxy-Server. Als Faustregel gilt, dass Sie die Einstellungen der Proxy-Verbindung Ihrer Bitdefender-Anwendung prüfen und konfigurieren sollten, falls Updates nicht funktionieren. Wenn Bitdefender sich aktualisieren kann, dann ist es richtig konfiguriert, um eine Verbindung mit dem Internet aufzubauen.

So können Sie Ihre Proxy-Einstellungen verwalten:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Einstellungen**.
2. Wechseln Sie zum Reiter **Erweitert**.
3. Aktivieren Sie die Option **Proxy-Server**.
4. Klicken Sie auf **Proxy-Änderung**.
5. Sie haben zwei Möglichkeiten, die Proxy-Einstellungen vorzunehmen:
   - **Proxy-Einstellungen aus Standard-Browser importieren** - Proxy-Einstellungen des aktuellen Benutzers, aus dem Standard-Browser importiert. Sollte ein Benutzername und Passwort nötig sein so geben Sie diesen in die dafür vorgesehenen Felder ein.

     Beachten Sie
     Bitdefender kann die Proxy-Einstellungen aus den gängigsten Browsern importieren, einschließlich der neuesten Versionen von Internet Explorer, Mozilla Firefox und Google Chrome.

- **Benutzerdefinierte Proxy-Einstellungen** - Proxy-Einstellungen, die Sie selbst konfigurieren können. Die folgenden Einstellungen müssen angegeben werden:
  - **Adresse** - Geben Sie die IP-Adresse des Proxy-Servers ein.
  - **Port** - Geben Sie den Port ein, über den Bitdefender die Verbindung zum Proxy-Server herstellt.
  - **Name** - Geben Sie einen für den Proxy-Server gültigen Benutzernamen ein.
  - **Passwort** - Geben Sie das Passwort für den zuvor angegebenen Benutzer ein.

6. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Bitdefender wird die verfügbaren Proxy-Einstellungen verwenden, bis die Lösung eine Verbindung mit dem Internet aufbauen kann.

10.5. Ist auf meinem System die 32- oder 64-Bit-Version von Windows installiert?

So können Sie ermitteln, ob Sie über ein 32-Bit- oder 64-Bit-Betriebssystem verfügen:

- In **Windows 7**:
  1. Klicken Sie auf **Start**.
  2. Finden Sie **Computer** im **Start**-Menü.
  3. Rechtsklicken Sie auf **Arbeitsplatz** und wählen Sie **Eigenschaften**.
  4. Unter **System** können Sie die Systeminformationen einsehen.
- In **Windows 8**:
  1. Finden Sie auf der Windows-Startseite den Eintrag **Computer** (z.B. durch die Eingabe von "Computer" auf der Startseite) und klicken Sie auf das entsprechende Symbol.

     Finden Sie unter **Windows 8.1 Dieser PC**.
  2. Wählen Sie im Menü unten **Eigenschaften**.
  3. Im Bereich System finden Sie Ihren Systemtyp.
- In **Windows 10**:

1. Geben Sie "System" in das Suchfeld in der Taskleiste ein und klicken Sie auf das entsprechende Symbol.
2. Im Bereich System finden Sie Informationen zu Ihrem Systemtyp.

10.6. Wie kann ich in Windows versteckte Objekte anzeigen?

Diese Schritte sind sinnvoll in den Fällen, in denen Sie es mit einer Bedrohungssituation zu tun haben und Sie infizierte Dateien, die eventuell verborgen sind, finden und entfernen müssen.

Gehen Sie folgendermaßen vor, um versteckte Objekte in Windows anzuzeigen:

1. Klicken Sie auf **Start** und öffnen Sie die **Systemsteuerung**.

   In **Windows 8 und Windows 8.1**: Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
2. Klicken Sie auf **Ordneroptionen**.
3. Gehen Sie auf den Reiter **Ansicht**.
4. Wählen Sie **Verborgene Dateien und Verzeichnisse anzeigen**.
5. Entfernen Sie den Haken bei **Erweiterungen bei bekannten Dateitypen ausblenden**.
6. Deaktivieren Sie **Geschützte Betriebssystemdateien verbergen**.
7. Klicken Sie auf **Anwenden** und danach auf **OK**.

In **Windows 10**:

1. Geben Sie "Alle Dateien und Ordner anzeigen" in das Suchfeld in der Taskleiste ein und klicken Sie auf das entsprechende Symbol.
2. Wählen Sie **Ausgeblendete Dateien, Ordner und Laufwerke anzeigen** aus.
3. Entfernen Sie den Haken bei **Erweiterungen bei bekannten Dateitypen ausblenden**.
4. Deaktivieren Sie **Geschützte Betriebssystemdateien verbergen**.
5. Klicken Sie auf **Anwenden** und danach auf **OK**.

10.7. Wie entferne ich andere Sicherheitslösungen?

Der Hauptgrund für den Einsatz einer Sicherheitslösung ist der Schutz und die Sicherheit Ihrer Daten. Aber was geschieht, wenn mehr als ein Sicherheitsprogramm auf demselben System läuft?

Wenn Sie mehr als eine Sicherheitslösung auf Ihrem Gerät verwenden, wird dadurch das System instabil. Das Bitdefender Antivirus Free-Installationsprogramm findet automatisch andere auf dem System installierte Sicherheits-Software und bietet an, diese zu deinstallieren.

Falls Sie weitere bereits auf dem PC installierte Sicherheitslösungen nicht während der Installation entfernt haben:

- In **Windows 7**:
  1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
  2. Warten Sie einen Moment, bis die Liste der installierten Software angezeigt wird.
  3. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.
  4. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.
- In **Windows 8 und Windows 8.1**:
  1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
  2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
  3. Warten Sie einen Moment, bis die Liste der installierten Software angezeigt wird.
  4. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.
  5. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.
- In **Windows 10**:
  1. Klicken Sie auf **Start** und danach auf Einstellungen.

2. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und danach auf **Apps**.
3. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.
4. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.
5. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.

Wenn es Ihnen nicht gelingt, weitere auf Ihrem Rechner installierte Sicherheits-Software zu entfernen, laden Sie sich das Deinstallations-Tool von der Website des entsprechenden Herstellers herunter oder wenden Sie sich direkt an den Hersteller für eine Deinstallationsanleitung.

10.8. Wie führe ich einen Neustart im abgesicherten Modus durch?

Der abgesicherte Modus ist ein diagnostischer Betriebsmodus, der hauptsächlich bei der Suche nach Fehlern zum Einsatz kommt, die den normalen Windows-Betrieb beeinträchtigen. Solche Probleme reichen von in Konflikt stehenden Treibern bis hin zu Bedrohungen, die Windows daran hindern, normal hochzufahren. Im abgesicherten Modus funktionieren nur einige wenige Anwendungen und Windows lädt nur die wichtigsten Treiber und ein Minimum an Betriebssystemkomponenten. Deshalb sind bei einer Verwendung von Windows im abgesicherten Modus die meisten Bedrohungen inaktiv und können einfach entfernt werden.

Start von Windows im abgesicherten Modus:

- In **Windows 7**:
  1. Starten Sie das Gerät neu.
  2. Drücken Sie wiederholt die **F8**-Taste, bevor Windows startet, um so Zugriff auf das Boot-Menü zu erhalten.
  3. Wählen Sie **Abgesicherter Modus** im Boot-Menü oder **Abgesicherter Modus mit Netzwerktreibern**, falls Sie Zugang zum Internet haben möchten.
  4. Drücken Sie die **Eingabetaste** und warten Sie, während Windows im abgesicherten Modus startet.

5. Dieser Vorgang endet mit einer Bestätigungsbenachrichtigung. Klicken Sie zur Bestätigung auf **OK**.
6. Um Windows normal zu starten, starten Sie einfach Ihr System neu.

- In **Windows 8, Windows 8.1 und Windows 10**:

1. Rufen Sie die **Systemkonfiguration** in Windows auf, indem Sie auf Ihrer Tastatur gleichzeitig die Tasten **Windows + R** drücken.
2. Geben Sie **msconfig** in das **Öffnen**-Dialogfeld ein und klicken Sie auf **OK**.
3. Wechseln Sie zum Reiter **Boot**.
4. Aktivieren Sie im Bereich **Startoptionen** das Kästchen **Sicherer Start**.
5. Klicken Sie auf **Netzwerk** und dann auf **OK**.
6. Im Fenster **Systemkonfiguration** werden Sie darüber informiert, dass Ihr System zur Übernahme der Änderungen neu gestartet werden muss. Klicken Sie auf **OK**.

   Ihr System wird im Abgesicherten Modus mit Netzwerktreibern neu gestartet.

Setzen Sie die Einstellungen zurück, um Ihr System im Normalen Modus neu zu starten. Starten Sie dazu den **Systemvorgang** erneut und deaktivieren Sie das Kästchen **Sicherer Start**. Klicken Sie auf **OK** und dann auf **Neustart**. Warten Sie, bis die neuen Einstellungen übernommen wurden.

DIE SICHERHEITSELEMENTE IM DETAIL

11. VIRENSCHUTZ

Bitdefender schützt Ihr Gerät vor allen Arten von Bedrohungen (Malware, Trojaner, Spyware, Rootkits etc.). Der Virenschutz, den Bitdefender bietet, lässt sich in zwei Kategorien einteilen:

- Zugriff-Scan - Verhindert, dass neue Bedrohungen auf Ihr System gelangen. Bitdefender wird z.B. ein Worddokument auf Malware scannen, wenn Sie es öffnen oder eine Email-Nachricht, wenn Sie diese empfangen.

  Der Zugriff-Scan stellt den Echtzeitschutz vor Bedrohungen sicher und ist damit ein grundlegender Bestandteil jedes Computer-Sicherheitsprogramms.

  Wichtig
  Um zu verhindern, dass Ihr Gerät durch Bedrohungen infiziert wird, sollte der **Zugriff-Scan** immer aktiviert bleiben.

- On-demand Prüfung - erkennt und entfernt die Bedrohung, die sich bereits auf dem System befindet. Hierbei handelt es sich um einen klassischen, durch den Benutzer gestarteten, Scan - Sie wählen das Laufwerk, Verzeichnis oder Datei, die Bitdefender scannen soll und Bitdefender scannt diese.

Bitdefender scannt automatisch alle Wechselmedien, die mit dem Gerät verbunden werden, um einen sicheren Zugriff zu garantieren. Weitere Informationen finden Sie im Kapitel *„Automatischer Scan von Wechselmedien“* (S. 72).

Erfahrene Benutzer können Scan-Ausnahmen konfigurieren, wenn Sie nicht möchten, dass bestimmte Dateien oder Dateitypen gescannt werden. Weitere Informationen finden Sie im Kapitel *„Konfigurieren der Scan-Ausnahmen“* (S. 74).

Wenn Bitdefender eine Bedrohung erkennt, versucht das Programm automatisch den Schad-Code der infizierten Datei zu entfernen und die Originaldatei wiederherzustellen. Diese Operation bezeichnet man als Desinfektion. Dateien, die nicht desinfiziert werden können, werden in die Quarantäne verschoben, um so die Infizierung einzudämmen. Weitere Informationen finden Sie im Kapitel *„Verwalten von Dateien in Quarantäne“* (S. 76).

Wenn Ihr Gerät durch Bedrohungen infiziert wurde, siehe *„Entfernung von Bedrohungen“* (S. 98).

11.1. Zugriff-Scans (Echtzeitschutz)

Bitdefender bietet durch die Prüfung aller aufgerufenen Dateien und E-Mail-Nachrichten Echtzeitschutz vor einer Vielzahl von Bedrohungen.

11.1.1. Aktivieren / Deaktivieren des Echtzeitschutzes

So können Sie den Echtzeitschutz vor Bedrohungen aktivieren oder deaktivieren:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Öffnen**.
3. Aktivieren oder deaktivieren Sie im Fenster **Erweitert** die Option **Bitdefender-Schild**.
4. Wenn Sie den Echtzeitschutz deaktivieren, wird ein Warnfenster angezeigt. Sie müssen Ihre Auswahl bestätigen, indem Sie im Menü wählen, wie lange der Echtzeitschutz deaktiviert bleiben soll. Sie können den Echtzeitschutz für 5, 15 oder 30 Minuten, 1 Stunde, dauerhaft oder bis zum Neustart des Systems deaktivieren. Der Echtzeitschutz wird automatisch nach Ablauf des festgelegten Zeitraums aktiviert.

Warnung
Hierbei handelt es sich um ein grobes Sicherheitsrisiko. Wir empfehlen den Echtzeitschutz so kurz wie möglich zu deaktivieren. Während der Echtzeitschutz deaktiviert ist, sind Sie nicht vor Bedrohungen geschützt.

11.1.2. Wiederherstellen der Standardeinstellungen

Die vorgegebenen Einstellungen zum Echtzeitschutz stellen einen guten Schutz gegen Bedrohungen bei nur minimaler Beeinträchtigung der Systemleistung sicher.

Um die vorgegebenen Echzeitschutz-Einstellungen wiederherzustellen:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.

2. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Öffnen**.
3. Scrollen Sie im Fenster **Erweitert** nach unten, bis Sie die Option **Erweiterte Einstellungen zurücksetzen** sehen. Wählen Sie diese Option aus, um die Virenschutzeinstellungen auf die Standardeinstellungen zurückzusetzen.

11.2. Bedarf-Scan

Die Aufgabe der Bitdefender-Software ist es sicherzustellen, dass es keine Bedrohungen auf Ihrem Gerät gibt. Dies wird erreicht, indem neue Bedrohungen ferngehalten und Ihre E-Mail-Nachrichten sowie alle heruntergeladenen oder auf Ihr Gerät kopierten Dateien sorgfältig gescannt werden.

Es besteht aber die Gefahr, dass eine Bedrohung bereits in Ihrem System lauert, bevor Sie Bitdefender installieren. Deshalb sollten Sie Ihr Gerät nach der Installation von Bitdefender auf bereits vorhandene Bedrohungen prüfen. Übrigens sollten Sie Ihr Gerät auch in Zukunft regelmäßig auf Bedrohungen prüfen.

Bedarf-Scans werden über Scan-Aufgaben ausgeführt. Die Scan-Aufgaben beinhalten die Scan-Optionen und die Objekte, die gescannt werden sollen. Sie können das Gerät jederzeit scannen, indem Sie die Standard-Aufgaben oder Ihre eigenen Scan-Aufgaben (benutzerdefinierte Aufgaben) ausführen. Wenn Sie bestimmte Bereiche Ihres Geräts scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierten Scan konfigurieren und ausführen.

11.2.1. Eine Datei oder einen Ordner auf Bedrohungen prüfen

Wenn Sie den Verdacht hegen, dass Dateien und Verzeichnisse infiziert sein könnten, sollten Sie einen Scan durchführen. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner, die/den Sie scannen möchten, wählen Sie **Bitdefender** und dann **Mit Bitdefender scannen**. Der Viren-Scan-Assistent wird angezeigt. Er führt Sie durch den Scan-Vorgang. Wenn der Scan beendet wurde, werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.

11.2.2. Durchführen von Quick Scans

Quick Scan setzt auf In-the-Cloud-Scans, um auf Ihrem System laufende Bedrohungen aufzuspüren. Die Ausführung eines Quick Scans dauert im

Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virenschutz-Scan in Anspruch nehmen würde.

So können Sie eine Quick Scan durchführen:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Öffnen**.
3. Klicken Sie im Fenster **Scans** neben **Quick Scan** auf die Schaltfläche **Scan starten**.
4. Folgen Sie den Anweisungen des Viren-Scan-Assistenten, um den Scan abzuschließen. Bitdefender wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen. Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

11.2.3. Durchführen von System-Scans

Der System-Scan prüft das gesamte Gerät auf alle Bedrohungsarten, die ein Sicherheitsrisiko darstellen, so zum Beispiel Malware, Spyware, Adware, Rootkits usw.

Beachten Sie
Da ein **System-Scan** das gesamte System scannt, kann er eine Weile dauern. Es empfiehlt sich daher, diese Aufgabe durchzuführen, wenn Sie das Gerät gerade nicht benötigen.

Bevor Sie einen System-Scan ausführen, sollten Sie Folgendes beachten:

- Stellen Sie sicher, dass die Datenbank mit den Bedrohungsinformationen in Bitdefender jederzeit auf dem neuesten Stand ist. Wenn die Bedrohungsprüfung auf Grundlage einer Datenbank mit veralteten Bedrohungsinformationen erfolgt, kann dies verhindern, dass Bitdefender neue Bedrohungen erkennt, die seit dem letzten Update gefunden wurden. Weitere Informationen finden Sie im Kapitel *„Bitdefender auf dem neuesten Stand halten“* (S. 32).
- Schließen Sie alle geöffneten Programme.

Wenn Sie bestimmte Bereiche Ihres Geräts scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierten Scan

konfigurieren und ausführen. Weitere Informationen finden Sie im Kapitel *„Benutzerdefinierte Scans durchführen“ (S. 64)*.

So können Sie einen System-Scan durchführen:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Öffnen**.
3. Klicken Sie im Fenster **Scans** neben **System-Scan** auf die Schaltfläche **Scan starten**.
4. Bei der ersten Durchführung eines System-Scans werden Sie mit der Funktion vertraut gemacht. Klicken zum Fortfahren auf **OK, verstanden**.
5. Folgen Sie den Anweisungen des Viren-Scan-Assistenten, um den Scan abzuschließen. Bitdefender wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen. Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

11.2.4. Benutzerdefinierte Scans durchführen

Im Fenster **Scans verwalten** können Sie Bitdefender so einrichten, dass Scans ausgeführt werden, wenn Sie glauben, dass Ihr Gerät eine Überprüfung auf mögliche Bedrohungen benötigt. Sie können wählen, ob Sie einen System-Scan oder einen Quick-Scan planen möchten, oder ob Sie einen benutzerdefinierten Scan nach Ihren Anforderungen erstellen möchten.

So können Sie einen benutzerdefinierten Scan im Detail konfigurieren:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Öffnen**.
3. Klicken Sie im Fenster **Scans** auf **+Scan erstellen**.
4. Geben Sie im Feld **Aufgabenname** einen Namen für den Scan ein, wählen Sie die Bereiche aus, die Sie scannen möchten, und klicken Sie auf **Weiter**.
5. Konfigurieren Sie diese allgemeinen Optionen:
   - **Nur Anwendungen scannen**. Sie können Bitdefender so konfigurieren, dass nur aufgerufene Apps gescannt werden.

- **Priorität der Scan-Aufgabe**. Sie können festlegen, wie sich ein Scan-Vorgang auf die Systemleistung auswirkt.
  - Auto - Die Priorität des Scan-Vorgangs hängt von der Systemaktivität ab. Um sicherzustellen, dass der Scan-Vorgang die Systemaktivität nicht beeinträchtigt, entscheidet Bitdefender, ob der Scan-Vorgang mit hoher oder niedriger Priorität ausgeführt wird.
  - Hoch - Die Priorität des Scan-Vorgangs wird als hoch festgelegt. Wenn Sie diese Option wählen, können andere Programme langsamer ausgeführt werden. So kann der Scan-Vorgang schneller abgeschlossen werden.
  - Niedrig - Die Priorität des Scan-Vorgangs wird als niedrig festgelegt. Wenn Sie diese Option wählen, können andere Programme schneller ausgeführt werden. So dauert es länger, bis der Scan-Vorgang abgeschlossen wird.
- **Aktionen nach dem Scan**. Wählen Sie die Aktion, die von Bitdefender durchgeführt werden soll, wenn keine Bedrohungen gefunden wurden:
  - Übersichtsfenster anzeigen
  - Gerät herunterfahren
  - Scan-Fenster schließen

6. Um die Scan-Optionen im Detail zu konfigurieren, klicken Sie auf **Erweiterte Optionen anzeigen**. Informationen zu den aufgeführten Scans finden Sie am Ende dieses Abschnitts.

   Klicken Sie auf **Weiter**.

7. Sie können bei Bedarf die Option **Scan-Aufgabe planen** aktivieren und dann festlegen, wann der von Ihnen erstellte benutzerdefinierte Scan gestartet werden soll.
   - Beim Systemstart
   - Täglich
   - Monatlich
   - Wöchentlich

   Wenn Sie Täglich, Monatlich oder Wöchentlich wählen, ziehen Sie den Regler entlang der Skala, um den gewünschten Zeitraum festzulegen, in dem der geplante Scan beginnen soll.

8. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Konfigurationsfenster zu schließen.

   Abhängig von den Bereichen, die gescannt werden sollen, kann der Scan einige Zeit in Anspruch nehmen. Wenn während des Scan-Vorgangs Bedrohungen gefunden werden, werden Sie aufgefordert, die Aktionen auszuwählen, die für die erkannten Dateien durchgeführt werden sollen.

Informationen zu den Scan-Optionen

Diese Informationen sind vielleicht nützlich:

- Wenn Ihnen bestimmte Begriffe nicht geläufig sind, schlagen Sie diese im Glossar nach. Sie könne auch durch eine Suche im Internet hilfreiche Informationen finden.
- **Auf potenziell unerwünschte Anwendungen prüfen.** Wählen Sie diese Option, um nach nicht erwünschten Anwendungen zu suchen. Bei einer potenziell unerwünschten Anwendung (PUA) oder einem potenziell unerwünschten Programm (PUP) handelt es sich um Software, die meist in Verbindung mit kostenloser Software installiert wird und danach Pop-up-Nachrichten anzeigt oder eine Symbolleiste im Standard-Browser installiert. Einige dieser Anwendungen und Programme verändern die Homepage oder die Suchmaschine, andere führen Hintergrundprozesse aus, die den PC verlangsamen, oder zeigen immer wieder Werbung an. Diese Programme können ohne Ihre Zustimmung installiert werden (wird auch als Adware bezeichnet) oder werden standardmäßig bei der Express-Installation mitinstalliert (werbeunterstützt).
- **Prüft den Inhalt von Archiven.** Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für Ihre Systemsicherheit. Die Bedrohung kann Ihr System nur dann beeinträchtigen, wenn die infizierten Datei aus einem Archiv extrahiert und ohne aktivierten Echtzeitschutz ausgeführt wird. Wir empfehlen jedoch, diese Option zu nutzen, um jegliche potentiellen Bedrohungen aufzuspüren und zu entfernen, auch wenn es sich nicht um unmittelbare Bedrohungen handelt.

  Ziehen Sie den Regler entlang der Skala, um Archive, die größer als ein bestimmter Wert in MB (Megabyte) sind, vom Scan auszuschließen.

  ### Beachten Sie
  Das Scannen archivierter Dateien erhöht die Gesamt-Scandauer und erfordert mehr Systemressourcen.

- **Nur neue und veränderte Dateien scannen.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.
- **Boot-Sektoren scannen.** Sie können Bitdefender einstellen, damit die Boot-Sektoren gescannt werden. Dieser Sektor der Festplatte beinhaltet den notwendigen Computercode um den Boot-Prozess zu starten. Wenn der Boot-Sektor durch eine Bedrohung infiziert wird, könnte das Laufwerk unzugänglich werden und es könnte Ihnen nicht mehr möglich sein, Ihr System zu starten und auf Ihre Daten zuzugreifen.
- **Speicher scannen.** Wählen Sie diese Option, um Programme zu scannen, die im Speicher Ihres Systems laufen.
- **Registrierung scannen.** Wählen Sie diese Option, um die Registrierungsschlüssel zu scannen. Die Windows-Registrierung ist eine Datenbank, in der Konfigurationseinstellungen und Optionen für die Windows-Betriebssystemkomponenten sowie für die installierten Anwendungen gespeichert sind.
- **Cookies scannen.** Wählen Sie diese Option, um die Cookies zu scannen, die von Browsern auf dem Gerät gespeichert werden.
- **Nach Keylogger prüfen.** Wählen Sie diese Option, um Ihr System auf Keylogger zu untersuchen. Keylogger zeichnen auf, was Sie auf Ihrer Tastatur tippen, und schicken dann via Internet Berichte an Hacker. Der Hacker kann über diese gestohlenen Daten sensible Informationen erfahren, so wie Kontonummern und Passwörter und kann Sie zu seinem eigenen Profit verwenden.

11.2.5. Viren-Scan-Assistent

Wann immer Sie einen Bedarf-Scan starten (z. B. indem Sie mit der rechten Maustaste auf einen Ordner klicken, dann Bitdefender und anschließend **Mit Bitdefender scannen** wählen), wird der Bitdefender-Viren-Scan-Assistent eingeblendet. Folgen Sie den Anweisungen des Assistenten, um den Scan-Prozess abzuschließen.

Beachten Sie

Falls der Scan-Assistent nicht erscheint, ist der Scan möglicherweise konfiguriert, im Hintergrund zu laufen. Sehen Sie nach dem

Prüffortschritticon im Systemtray. Sie können dieses Objekt anklicken um das Scan-Fenster zu öffnen und so den Scan-Fortschritt zu sehen.

Schritt 1 - Führen Sie den Scan durch

Bitdefender startet den Scan der aus gewählten Dateien und Verzeichnisse. Sie erhalten Echtzeitinformationen über den Scan-Status sowie Scan-Statistiken (einschließlich der bisherigen Laufzeit, einer Einschätzung der verbleibenden Laufzeit und der Anzahl der erkannten Bedrohungen).

Bitte warten Sie, bis Bitdefender den Scan beendet hat. Der Scan-Vorgang kann, abhängig von der Größe Ihrer Festplatte, eine Weile dauern.

Einen Scan anhalten oder unterbrechen. Sie können den Scan-Vorgang jederzeit durch einen Klick auf **STOPP** abbrechen. Sie gelangen dann direkt zum letzten Schritt des Assistenten. Um den Scan-Vorgang vorübergehend anzuhalten, klicken Sie einfach auf **PAUSE**. Um den Scan-Vorgang fortzusetzen klicken Sie auf **FORTSETZEN** .

Passwortgeschützte Archive. Wird ein passwortgeschütztes Archiv gefunden, werden Sie, abhängig von den Scan-Einstellungen, um die Eingabe des Passwortes gebeten. Mit Passwort geschützte Archive können nicht gescannt werden, außer wenn Sie das Passwort angeben. Die folgenden Optionen stehen zur Verfügung:

- **Passwort.** Wenn Sie möchten, dass Bitdefender Archive scannt, wählen Sie diese Option aus und geben das Passwort an. Falls Sie das Passwort nicht kennen, wählen Sie eine der anderen Optionen.
- **Nicht nach einem Passwort fragen und dieses Objekt beim Scan überspringen.** Wählen Sie diese Option um das Scannen diesen Archivs zu überspringen.
- **Alle passwortgeschützten Dateien beim Scan überspringen.** Wählen Sie diese Option, falls Sie nicht über passwortgeschützte Archive informiert werden möchten. Bitdefender kann diese Dateien und Objekte nicht scannen, erstellt aber einen Eintrag im Scan-Protokoll.

Wählen Sie die gewünschte Option aus und klicken Sie auf **OK**, um den Scan fortzusetzen.

Schritt 2 - Wählen Sie entsprechende Aktionen aus

Wenn der Scan beendet wurde, werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.

Beachten Sie

Wenn Sie einen Quick Scan oder einen System-Scan durchführen, wird Bitdefender während des Scans automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen. Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

Die infizierten Objekte werden nach Bedrohung sortiert in Gruppen angezeigt. Klicken Sie auf den Link, der der Bedrohung entspricht, um weitere Informationen über die infizierten Objekte zu erhalten.

Sie können eine umfassende Aktion für alle Probleme auswählen oder Sie können einzelne Aktionen für Problemgruppen auswählen. Eine oder mehrere der folgenden Optionen können im Menu erscheinen:

Aktionen ausführen

Bitdefender wird je nach Art der infizierten Datei die empfohlenen Aktionen ausführen:

- **Infizierte Dateien.** Dateien, die als infiziert erkannt werden, stimmen mit einer in der Bitdefender-Datenbank gefunden Bedrohungsinformationen überein. Bitdefender wird automatisch versuchen, den Schad-Code aus der infizierten Datei zu entfernen und die Originaldatei zu rekonstruieren. Diese Operation bezeichnet man als Desinfektion.

  Dateien, die nicht desinfiziert werden können, werden in die Quarantäne verschoben, um so die Infizierung einzudämmen. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko. Weitere Informationen finden Sie im Kapitel *„Verwalten von Dateien in Quarantäne“ (S. 76)*.

Wichtig

Bestimmte Bedrohungsarten können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

- **Verdächtige Dateien.** Dateien werden von der heuristischen Analyse als verdächtig klassifiziert. Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist. Sie werden in Quarantäne verschoben, um eine mögliche Infektion zu verhindern.

  Dateien in Quarantäne werden standardmäßig an die Bitdefender-Labore geschickt, damit Sie dort von den Bitdefender-Bedrohungsforschern analysiert werden können. Wird das Vorhandensein einer Bedrohung bestätigt, werden die Informationen per Update aktualisiert, damit die Bedrohung entfernt werden kann.

- **Archive mit infizierten Dateien.**
  - Archive, die nur infizierte Dateien enthalten, werden automatisch gelöscht.
  - Wenn ein Archiv sowohl infizierte als auch nicht infizierte Dateien enthält, wird Bitdefender versuchen, die infizierten Dateien zu löschen, vorausgesetzt, dass das Archiv mit den nicht infizierten Dateien wieder rekonstruiert werden kann. Wenn das Archiv nicht rekonstruiert werden kann, werden Sie benachrichtigt, dass keine Aktion durchgeführt werden kann, weil die Gefahr besteht, dass nicht infizierte Dateien verloren gehen.

Löschen

Infizierte Dateien werden von der Festplatte entfernt.

Falls infizierte Dateien zusammen mit nicht infizierten Dateien in einem Archiv gespeichert sind, wird Bitdefender versuchen, die infizierten Dateien zu löschen und das Archiv mit den nicht infizierten Dateien zu rekonstruieren. Wenn das Archiv nicht rekonstruiert werden kann, werden Sie benachrichtigt, dass keine Aktion durchgeführt werden kann, weil die Gefahr besteht, dass nicht infizierte Dateien verloren gehen.

Keine Aktion ausführen

Es wird keine Aktion für die infizierte Dateien ausgeführt. Nachdem der Scan-Vorgang beendet wurde, können Sie das Scan-Protokoll öffnen um Informationen über diese Dateien anzuzeigen.

Klicken Sie auf **Fortfahren** um die festgelegten Aktionen anzuwenden.

Schritt 3 - Zusammenfassung

Wenn Bitdefender die Probleme gelöst hat, wird eine Zusammenfassung der Scan-Ergebnisse in einem neuen Fenster angezeigt. Falls Sie umfangreichere Informationen zum Scan-Prozess möchten, klicken Sie auf **LOGDATEI ANZEIGEN**.

Wichtig

In den meisten Fällen desinfiziert Bitdefender erfolgreich die aufgespürten infizierten Dateien oder er isoliert die Infektion. Dennoch gibt es Probleme, die nicht automatisch gelöst werden können. Bitte starten Sie Ihr System neu, wenn Sie dazu aufgefordert werden, damit der Bereinigungsprozess abgeschlossen werden kann. Weitere Informationen und eine Anleitung, wie Sie eine Bedrohung manuell entfernen können, finden Sie im Kapitel *„Entfernung von Bedrohungen“* (S. 98).

11.2.6. Scan-Protokolle lesen

Bei jedem Scan wird ein Scan-Protokoll erstellt, und Bitdefender zeichnet die gefundenen Probleme im Fenster Virenschutz auf. Der Bericht enthält detaillierte Informationen über den Scan-Vorgang, so wie Scan-Optionen, das Scan-Ziel, die gefundenen Bedrohungen und die Aktionen, die für diese Bedrohungen ausgeführt wurden.

Sobald der Scan beendet ist, können Sie das Scan-Protokoll direkt aus dem Scan-Assistenten heraus öffnen, indem Sie auf **PROTOKOLL ANZEIGEN** klicken.

So können Sie ein Scan-Protokoll oder gefundene Infektionen auch später anzeigen:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Benachrichtigungen**.
2. Wählen Sie unter dem Reiter **Alle** die Benachrichtigung bezüglich des neuesten Scans aus.

   Hier können Sie alle Ereignisse des Bedrohungs-Scans finden, einschließlich der Bedrohungen, die während Zugriff-Scans und vom Benutzer gestarteten Scans entdeckt wurden. Dazu kommen Statusänderungen für automatische Scans.

3. In der Benachrichtigungsliste können Sie überprüfen, welche Scans kürzlich durchgeführt wurden. Klicken Sie auf eine Benachrichtigung, um mehr darüber zu erfahren.
4. Um das Scan-Protokoll zu öffnen, klicken Sie auf **Protokoll anzeigen**.

11.3. Automatischer Scan von Wechselmedien

Bitdefender erkennt automatisch, wenn Sie Wechselmedien mit Ihrem Gerät verbinden und scannt diese im Hintergrund, wenn die Auto-Scan-Option aktiviert wurde. Dies ist empfohlen, um die Infizierung Ihres Geräts durch Bedrohungen zu verhindern.

Entdeckte Geräte fallen in eine dieser Kategorien:

- CDs/DVDs
- Speichersticks, wie z. B. Flash Pens oder externe Festplatten
- verbundene (entfernte) Netzlaufwerke

Sie können den automatischen Scan der Speichermedien eigens für jede Kategorie konfigurieren. Der automatische Scan der abgebildeten Netzlaufwerke ist standardmäßig deaktiviert.

11.3.1. Wie funktioniert es?

Wenn ein Wechseldatenträger erkannt wird, beginnt Bitdefender diesen auf Bedrohungen zu prüfen (vorausgesetzt, dass der automatische Scan für diesen Gerätetyp aktiviert ist). Ein Pop-up-Fenster wird Sie darüber informieren, dass ein neues Gerät erkannt wurde und dass es derzeit gescannt wird.

Das Bitdefender-Scan-Symbol erscheint in der Task-Leiste. Sie können dieses Objekt anklicken um das Scan-Fenster zu öffnen und so den Scan-Fortschritt zu sehen.

Sobald der Scan abgeschlossen ist, wird das Fenster mit den Scan-Ergebnissen angezeigt, um Sie darüber zu informieren, ob Sie die Dateien auf dem Wechselmedium gefahrlos aufrufen können.

In den meisten Fällen entfernt Bitdefender erkannte Bedrohungen automatisch oder isoliert infizierte Dateien in der Quarantäne. Sollte es nach dem Scan noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

Beachten Sie

Beachten Sie, dass keine Aktion gegen infizierte oder verdächtige Dateien auf CDs/DVDs vorgenommen werden kann. Ähnlich können keine Aktionen gegen infizierte oder verdächtige Dateien auf Netzlaufwerken vorgenommen werden, wenn Sie nicht die entsprechenden Freigaben haben.

Diese Informationen könnten sich als hilfreich erweisen:

- Bitte gehen Sie vorsichtig vor, wenn Sie eine CD oder DVD nutzen, die mit Bedrohungen infiziert ist, da diese nicht von dem Datenträger entfernt werden kann (diese Medien sind schreibgeschützt). Stellen Sie sicher, dass der Echtzeitschutz aktiviert ist, um zu verhindern, dass Bedrohungen auf Ihr System gelangen. Es empfiehlt sich, wichtige Daten vom Datenträger auf Ihr System zu kopieren und den Datenträger dann zu entsorgen.
- Es kann vorkommen, dass Bitdefender nicht in der Lage ist, Bedrohungen aus juristischen oder technischen Gründen aus bestimmten Dateien zu entfernen. Ein Beispiel hierfür sind Dateien, die mithilfe von proprietären Technologien archiviert wurden (der Grund dafür ist, dass das Archiv nicht korrekt wiederhergestellt werden kann).

  Eine Anleitung zum Umgang mit Bedrohungen finden Sie im Kapitel *„Entfernung von Bedrohungen“* (S. 98).

11.3.2. Verwalten des Scans für Wechselmedien

So können Sie Wechselmedien automatisch scannen:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Öffnen**.
3. Rufen Sie das Fenster **Einstellungen** auf.

Die Prüfoptionen sind für bestmögliche Enteckungsraten vorkonfiguriert. Wenn infizierte Dateien erkannt werden, wird Bitdefender versuchen, diese zu desinfizieren (d. h. den Schad-Code zu entfernen) oder in die Quarantäne zu verschieben. Sollten beide Maßnahmen fehlschlagen, können Sie im Assistenten für den Virenschutz-Scan andere Aktionen für die infizierten Dateien festlegen. Die Prüfoptionen sind standartisiert, sie können daher nicht geändert werden.

Um den bestmöglichen Schutz zu garantieren, empfiehlt es sich, die **Auto-Scan-Option** für alle Arten von Wechselmedien zu aktivieren.

11.4. Konfigurieren der Scan-Ausnahmen

Mit Bitdefender können Sie bestimmte Dateien, Ordner oder Dateiendungen vom Scan ausnehmen. Diese Funktion soll verhindern, dass Sie bei Ihrer Arbeit gestört werden und kann zudem dabei helfen, die Systemleistung zu verbessern. Ausnahmen sollten nur von Benutzern genutzt werden, die erfahren im Umgang mit Computern sind oder wenn dies von einem Bitdefender-Mitarbeiter empfohlen wurde.

Sie können Ausnahmen so konfigurieren, dass sie für Zugriff-Scans, Bedarf-Scans oder beide Arten von Scans gelten. Die ausgenommenen Objekte werden nicht geprüft, egal ob der Zugriff von Ihnen oder von einem Programm erfolgt.

Beachten Sie

Ausnahmen werden bei Kontext-Scans NICHT berücksichtigt. Kontextprüfung ist eine Art von On-Demand-Scan: Rechtsklicken Sie auf die zu scannende Datei oder das Verzeichnis und wählen Sie **Mit Bitdefender scannen**.

11.4.1. Dateien und Ordner vom Scan ausnehmen

So können Sie bestimmte Dateien und Ordner vom Scan ausnehmen:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Öffnen**.
3. Klicken Sie im Fenster **Einstellungen** auf **Ausnahmen verwalten**.
4. Klicken Sie auf **+Ausnahme hinzufügen**.
5. Geben Sie den Pfad des Ordners, den Sie vom Scan ausnehmen möchten, in das entsprechende Feld ein.

   Alternativ können Sie zu dem Ordner navigieren, indem Sie rechts in der Benutzeroberfläche auf die Schaltfläche "Durchsuchen" klicken, ihn auswählen und dann auf **OK** klicken.
6. Aktivieren Sie den Schalter neben der Schutzfunktion, durch die der Ordner nicht gescannt werden soll. Sie haben drei Optionen:
   - Virenschutz
   - Online-Gefahrenabwehr

- Erweiterte Gefahrenabwehr

7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Fenster zu schließen.

11.4.2. Dateiendungen vom Scan ausnehmen

Wenn Sie eine Dateiendung vom Scan ausnehmen, wird Bitdefender Dateien mit dieser Endung unabhängig von ihrem Speicherort nicht mehr scannen. Die Ausnahme bezieht sich auch auf Dateien auf Wechselmedien, wie zum Beispiel CDs, DVDs, USB-Sticks oder Netzlaufwerke.

Wichtig
Lassen Sie Vorsichtig walten, wenn Sie Dateiendung vom Scan ausnehmen, da solche Ausnahmen Ihr Gerät anfällig für Bedrohungen machen können.

So können Sie Dateierweiterungen vom Scan ausnehmen:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Öffnen**.
3. Klicken Sie im Fenster **Einstellungen** auf **Ausnahmen verwalten**.
4. Klicken Sie auf **+Ausnahme hinzufügen**.
5. Geben Sie die Dateiendungen, die vom Scannen ausgenommen werden sollen, mit einem Punkt davor ein. Trennen Sie einzelne Endungen mit einem Semikolon (;).

   txt;avi;jpg

6. Aktivieren Sie den Schalter neben der Schutzfunktion, durch die die Dateiendung nicht gescannt werden soll.
7. Klicken Sie auf **Speichern**.

11.4.3. Verwalten der Scan-Ausnahmen

Werden die konfigurierten Scan-Ausnahmen nicht mehr benötigt, empfehlen wir, diese zu löschen oder die Scan-Ausnahmen zu deaktivieren.

So können Sie die Scan-Ausnahmen verwalten:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.

2. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Öffnen**.
3. Klicken Sie im Fenster **Einstellungen** auf **Ausnahmen verwalten**. Es wird eine Liste mit allen von Ihnen festgelegten Ausnahmen angezeigt.
4. Um Scan-Ausnahmen zu entfernen oder zu bearbeiten, klicken Sie auf die jeweiligen Schaltflächen. Gehen Sie wie folgt vor:
   - Klicken Sie zum Entfernen eines Eintrags aus der Liste auf die -Schaltfläche neben dem Eintrag.
   - Klicken Sie zum Bearbeiten eines Eintrags aus der Tabelle auf die Schaltfläche **Bearbeiten** neben dem Eintrag. Ein neues Fenster wird angezeigt. Hier können Sie nach Bedarf festlegen, welche Dateiendungen oder -pfade von welcher Schutzfunktion ausgeschlossen werden sollen. Führen Sie die notwendigen Änderungen durch und klicken Sie dann auf **Ändern**.

11.5. Verwalten von Dateien in Quarantäne

Mit Bedrohungen infizierte Dateien, die nicht desinfiziert werden können, sowie verdächtige Dateien werden von Bitdefender in einem sicheren Bereich isoliert, der sogenannten Quarantäne. Bedrohungen in Quarantäne können keinen Schaden anrichten, da sie dort nicht geöffnet oder ausgeführt werden können.

Dateien in Quarantäne werden standardmäßig an die Bitdefender-Labore geschickt, damit Sie dort von den Bitdefender-Bedrohungsforschern analysiert werden können. Wird das Vorhandensein einer Bedrohung bestätigt, werden die Informationen per Update aktualisiert, damit die Bedrohung entfernt werden kann.

Zudem werden nach jedem Update der Datenbank mit den Bedrohungsinformationen die Dateien in der Quarantäne von Bitdefender gescannt. Gesäuberte Dateien werden automatisch an ihren Ursprungsort zurück gelegt.

So können Sie die Dateien in der Quarantäne einsehen und verwalten:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Öffnen**.
3. Rufen Sie das Fenster **Einstellungen** auf.

Hier finden Sie den Namen der Dateien in Quarantäne, ihren ursprünglichen Speicherort sowie den Namen der gefundenen Bedrohungen.

4. Dateien in Quarantäne werden von Bitdefender in Übereinstimmung mit den Standardeinstellungen für die Quarantäne automatisch verwaltet.

   Sie können die Quarantäneeinstellungen nach einem Klick auf **Einstellungen anzeigen** an Ihre Anforderungen anpassen, dies wird aber nicht empfohlen.

   Klicken Sie auf die Schalter, um das Folgende zu aktivieren oder deaktivieren:

   Nach Update der Bedrohungsinformationen erneut scannen
   Lassen Sie diese Option aktiviert, um Dateien in Quarantäne automatisch nach jedem Update der Bedrohungsinformationen zu scannen. Gesäuberte Dateien werden automatisch an ihren Ursprungsort zurück gelegt.

   Inhalte löschen, die älter als 30 Tage sind
   Dateien in Quarantäne, die älter als 30 Tage sind, werden automatisch gelöscht.

   Ausnahmen für wiederhergestellte Dateien erstellen
   Dateien, die Sie aus der Quarantäne wiederherstellen, werden ohne Reparatur an Ihren ursprünglichen Speicherort verschoben und bei zukünftigen Scans automatisch übersprungen.

5. Um eine Quarantäne-Datei zu löschen, markieren Sie diese und klicken dann auf den Button **Löschen**. Wenn Sie eine Quarantäne-Datei am ursprünglichen Speicherort wiederherstellen möchten, klicken Sie zuerst auf die Datei und dann auf **Wiederherstellen**.

12. ERWEITERTE GEFAHRENABWEHR

Die Bitdefender Erweiterte Gefahrenabwehr ist eine innovative und vorbeugende Erkennungstechnologie, die hoch entwickelte heuristische Methoden nutzt, um Ransomware und mögliche neue Bedrohungen in Echtzeit zu erkennen.

Die Erweiterte Gefahrenabwehr überwacht durchgehend alle auf Ihrem Gerät laufenden Anwendungen auf Aktionen, die auf Bedrohungen hindeuten. Jede einzelne dieser Aktionen erhält einen Wert, und jeder Prozess erhält so einen aggregierten Gesamtwert.

Als Sicherheitsmaßnahme werden Sie jedes Mal benachrichtigt, wenn Bedrohungen und potenziell gefährliche Prozesse erkannt und blockiert werden.

12.1. Aktivieren oder Deaktivieren der Advanced Threat Defense

So aktivieren oder deaktivieren Sie die Advanced Threat Defense:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Klicken Sie im Bereich **ADVANCED THREAT DEFENSE** auf **Öffnen**.
3. Rufen Sie das Fenster **Einstellungen** auf und klicken Sie auf den Schalter neben **Bitdefender Erweiterte Gefahrenabwehr**.

> **Beachten Sie**
> Zum Schutz Ihrer Systeme vor Ransomware und anderen Bedrohungen empfehlen wir Ihnen, die Erweiterte Gefahrenabwehr nicht über einen längeren Zeitraum zu deaktivieren.

12.2. Einsehen von erkannten schädlichen Angriffen

Werden Bedrohungen oder potenziell schädliche Angriffe erkannt, werden diese von Bitdefender umgehend blockiert, um eine Infektion Ihres Geräts durch Ransomware oder andere Malware zu verhindern. Gehen Sie wie folgt vor, um eine Liste der erkannten schädlichen Angriffe einzusehen:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.

2. Klicken Sie im Bereich **ADVANCED THREAT DEFENSE** auf **Öffnen**.
3. Rufen Sie das Fenster **Threat Defense** auf.

   Alle in den vergangenen 90 Tagen erkannten Angriffe werden angezeigt. Klicken Sie auf den entsprechenden Eintrag, um weitere Details zum erkannten Ransomware-Typ und den Dateipfad des schädlichen Prozesses anzuzeigen. Hier können Sie auch einsehen, ob die Desinfektion erfolgreich war.

12.3. Hinzufügen von Prozessen zu den Ausnahmen

Sie können Ausnahmeregeln für vertrauenswürdige Anwendungen festlegen, damit die Erweiterte Gefahrenabwehr diese nicht blockiert, wenn ihr Verhalten auf eine Bedrohung hindeutet.

So können Sie Prozesse zur Ausnahmeliste der Erweiterten Gefahrenabwehr hinzufügen:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Klicken Sie im Bereich **ADVANCED THREAT DEFENSE** auf **Öffnen**.
3. Klicken Sie im Fenster **Einstellungen** auf **Ausnahmen verwalten**.
4. Klicken Sie auf **+Ausnahme hinzufügen**.
5. Geben Sie den Pfad des Ordners, den Sie vom Scan ausnehmen möchten, in das entsprechende Feld ein.

   Alternativ können Sie zu der ausführbaren Datei navigieren, indem Sie rechts in der Benutzeroberfläche auf die Schaltfläche "Durchsuchen" klicken, sie auswählen und dann auf **OK** klicken.
6. Aktivieren Sie den Schalter neben **Erweiterte Gefahrenabwehr**.
7. Klicken Sie auf **Speichern**.

12.4. Exploits gefunden

Hacker nutzen zum Eindringen in Systeme häufig bestimmte Fehler oder Schwachstellen in Computersoftware (Anwendungen oder Plug-ins) und Hardware aus. Um Ihr Gerät von derartigen Angriffen zu schützen, die sich in aller Regel sehr schnell ausbreiten, verwendet Bitdefender die neuesten Technologien zur Abwehr von Exploits.

Aktivieren oder Deaktivieren der Exploit-Erkennung

So können Sie die Exploit-Erkennung aktivieren oder deaktivieren:

- Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
- Klicken Sie im Bereich **ADVANCED THREAT DEFENSE** auf **Öffnen**.
- Rufen Sie das Fenster **Einstellungen** auf und klicken Sie auf den Schalter neben **Exploit-Erkennung**, um die Funktion zu aktivieren oder deaktivieren.

Beachten Sie

Die Option zur Exploit-Erkennung ist standardmäßig aktiviert.

13. ONLINE-GEFAHRENABWEHR

De Bitdefender-Online-Gefahrenabwehr lässt Sie sicher im Netz surfen, indem sie Sie vor potenziell schädlichen Seiten warnt.

Bitdefender bietet Echtzeit-Online-Gefahrenabwehr für:

- Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari
- Bitdefender Safepay™
- Opera

So können Sie die Einstellungen der Online-Gefahrenabwehr konfigurieren:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Klicken Sie im Bereich **ONLINE-GEFAHRENABWEHR** auf **Einstellungen**.

Klicken Sie im Bereich **Internet-Schutz** zur Aktivierung oder Deaktivierung auf die entsprechenden Schalter:

- Die Prävention von Internetangriffen blockiert Bedrohungen aus dem Internet, so zum Beispiel auch Drive-by-Downloads.
- Suchberater, eine Komponente, die Ihre Suchmaschinentreffer und Links auf Seiten sozialer Netzwerke analysiert und bewertet. Die Bewertung wird durch ein Symbol neben dem Link oder Treffer angezeigt:

  Sie sollten diese Webseite nicht aufrufen.

  Diese Webseite könnte gefährliche Inhalte haben. Seien Sie vorsichtig, wenn Sie sie dennoch aufrufen möchten.

  Diese Seite ist sicher.

  Der Suchberater anaylsiert die Treffer der folgenden Internet-Suchmaschinen:
  - Google
  - Yahoo!
  - Bing
  - Baidu

Der Suchberater bewertet Links, die auf den folgenden sozialen Netzwerken im Internet veröffentlicht werden:
- Facebook
- 109

- Verschlüsselter Web-Scan.

  Gute durchdachte Angriffsversuche könnten den sicheren Datenverkehr für sich zu nutzen, um ihre Opfer zu täuschen. Wir empfehlen daher, die Option Verschlüsselter Web-Scan aktiviert zu lassen.

- Betrugsschutz.
- Phishing-Schutz.

Sie können eine Liste mit Websites, Domains und IP-Adressen anlegen, die von den Bitdefender-Engines für den Bedrohungs-, Phishing- und Betrugsschutz nicht gescannt werden sollen. Die Liste sollte nur Websites, Domänen und IP-Adressen enthalten, denen Sie uneingeschränkt vertrauen.

So können Sie mit der Online-Gefahrenabwehr in Bitdefender Websites, Domains und IP-Adressen konfigurieren und verwalten:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Klicken Sie im Bereich **ONLINE-GEFAHRENABWEHR** auf **Einstellungen**.
3. Klicken Sie auf **Ausnahmen verwalten**.
4. Klicken Sie auf **+Ausnahme hinzufügen**.
5. Geben Sie in das entsprechende Feld den Namen der Website, den Namen der Domain oder die IP-Adresse ein, die Sie zu den Ausnahmen hinzufügen möchten.
6. Klicken Sie auf den Schalter neben **Online-Gefahrenabwehr**.
7. Klicken Sie zum Entfernen eines Eintrags aus der Liste auf die -Schaltfläche neben dem Eintrag.

   Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Fenster zu schließen.

13.1. Bitdefender-Benachrichtigungen im Browser

Wenn Sie versuchen eine Website aufzurufen, die als unsicher eingestuft wurde, wird die entsprechende Website blockiert und eine Warnseite wird in Ihrem Browser angezeigt.

Die Seite enthält Informationen wie zum Beispiel die URL der Website und die erkannte Bedrohung.

Sie müssen entscheiden, wie Sie fortfahren möchten. Die folgenden Optionen stehen zur Verfügung:

- Verlassen Sie die Website mit einem Klick auf **ICH GEHE LIEBER AUF NUMMER SICHER**.
- Rufen Sie die Website trotz der Warnung auf, indem Sie auf **Ich bin mir der Risiken bewusst und möchte trotzdem fortfahren** klicken.
- Wenn Sie sich sicher sind, dass die erkannte Website sicher ist, klicken Sie auf **SENDEN**, um Sie zu den Ausnahmen hinzuzufügen. Wir empfehlen Ihnen, nur Websites hinzuzufügen, denen Sie uneingeschränkt vertrauen.

PROBLEMLÖSUNG

14. VERBREITETE PROBLEME BEHEBEN

In diesem Kapitel werden einige Probleme, die Ihnen bei der Verwendung von Bitdefender begegnen können, erläutert. Zudem finden Sie hier Lösungsvorschläge für diese Probleme. Die meisten dieser Probleme können über eine passende Konfiguration der Produkteinstellungen gelöst werden.

Wenn Sie Ihr Problem hier nicht finden oder wenn die vorgeschlagene Lösung nicht zum Erfolg führt, können Sie den technischen Kundendienst von Bitdefender wie in Kapitel *„Hilfe anfordern“* (S. 106) beschrieben, kontaktieren.

14.1. Mein System scheint langsamer zu sein

Nach der Installation einer Sicherheitssoftware ist eine geringfügige Verlangsamung des Systems bis zu einem gewissen Grad normal.

Wenn Sie eine erhebliche Systemverlangsamung feststellen, kann dies folgende Ursachen haben:

- **Bitdefender ist nicht die einzige auf Ihrem System installierte Sicherheits-Software.**

  Obwohl Bitdefender bereits auf Ihrem System installierte Sicherheitsprogramme während der Installation sucht und entfernt, empfehlen wir dennoch, jede andere Sicherheitslösung von Ihrem Rechner zu entfernen, bevor Sie die Installation von Bitdefender starten. Weitere

Informationen finden Sie im Kapitel *„Wie entferne ich andere Sicherheitslösungen?“* (S. 56).

- **Die Systemvoraussetzungen für die Ausführung von Bitdefender sind nicht erfüllt.**

  Wenn Ihr Gerät die Systemvoraussetzungen nicht erfüllt, verlangsamt dies Ihr System, insbesondere dann, wenn mehrere Anwendungen gleichzeitig laufen. Weitere Informationen finden Sie im Kapitel *„Systemanforderungen“* (S. 3).

- **Sie haben Apps installiert, die Sie nicht verwenden**.

  Auf jedem Gerät sind Programme oder Anwendungen installiert, die Sie nicht verwenden. Im Hintergrund laufen viele unerwünschte Programme, die Speicherplatz und Arbeitsspeicher beanspruchen. Wenn Sie ein Programm nicht nutzen, deinstallieren Sie es. Das gilt auch für vorinstallierte Software oder Testversionen, die Sie nicht wieder entfernt haben.

  Wichtig
  Wenn Sie glauben, dass ein Programm oder eine Anwendung ein wichtiger Bestandteil Ihres Betriebssystems ist, entfernen Sie es nicht und wenden Sie sich an den Bitdefender-Kundendienst.

- **Ihr System ist vielleicht infiziert**.

  Die Geschwindigkeit und das allgemeine Verhalten Ihres Systems kann auch durch Bedrohungen beeinträchtigt werden. Spyware, Malware, Trojaner und Adware wirken sich negativ auf Ihre Geräteleistung aus. Stellen Sie sicher, dass Ihr System regelmäßig gescannt wird, mindestens einmal pro Woche. Es empfiehlt sich, einen Bitdefender-System-Scan durchzuführen, da so nach allen Bedrohungsarten gesucht wird, die die Sicherheit Ihres Systems gefährden.

  So können Sie einen System-Scan starten:

  1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
  2. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Öffnen**.
  3. Klicken Sie im Fenster **Scans** neben **System-Scan** auf die Schaltfläche **Scan starten**.
  4. Befolgen Sie die Anweisungen des Assistenten.

14.2. Der Scan startet nicht

Dieses Problem kann folgende Ursachen haben:

- **Eine vorherige Installation von Bitdefender wurde nicht vollständig entfernt oder es handelt sich um eine fehlerhafte Bitdefender-Installation**.

  Installieren Sie Bitdefender in diesem Fall neu:

  - In **Windows 7**:
    1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
    2. Suchen Sie **Bitdefender Antivirus Free** und wählen Sie **Deinstallieren**.
    3. Klicken Sie im angezeigten Fenster auf **NEU INSTALLIEREN**.
    4. Warten Sie, bis die Neuinstallation abgeschlossen ist und starten Sie Ihr System neu.
  - In **Windows 8 und Windows 8.1**:
    1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
    2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
    3. Suchen Sie **Bitdefender Antivirus Free** und wählen Sie **Deinstallieren**.
    4. Klicken Sie im angezeigten Fenster auf **NEU INSTALLIEREN**.
    5. Warten Sie, bis die Neuinstallation abgeschlossen ist und starten Sie Ihr System neu.
  - In **Windows 10**:
    1. Klicken Sie auf **Start** und danach auf Einstellungen.
    2. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie danach auf **Installierte Anwendungen**.
    3. Suchen Sie **Bitdefender Antivirus Free** und wählen Sie **Deinstallieren**.
    4. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.
    5. Klicken Sie im angezeigten Fenster auf **NEU INSTALLIEREN**.

6. Warten Sie, bis die Neuinstallation abgeschlossen ist und starten Sie Ihr System neu.

> **Beachten Sie**
> Wenn Sie bei der Neuinstallation wie hier beschrieben vorgehen, werden Ihre benutzerdefinierte Einstellungen gespeichert und sind im neu installierten Produkt wieder verfügbar. Weitere Einstellungen werden unter Umständen wieder auf die Standardkonfiguration zurückgesetzt.

- **Bitdefender ist nicht die einzige auf Ihrem System installierte Sicherheits-Software**.

  In diesem Fall:

  1. Entfernen Sie die andere Sicherheitslösung. Weitere Informationen finden Sie im Kapitel *„Wie entferne ich andere Sicherheitslösungen?“ (S. 56)*.
  2. Bitdefender neu installieren:
     - In **Windows 7**:
       a. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
       b. Suchen Sie **Bitdefender Antivirus Free** und wählen Sie **Deinstallieren**.
       c. Klicken Sie im angezeigten Fenster auf **NEU INSTALLIEREN**.
       d. Warten Sie, bis die Neuinstallation abgeschlossen ist und starten Sie Ihr System neu.
     - In **Windows 8 und Windows 8.1**:
       a. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
       b. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
       c. Suchen Sie **Bitdefender Antivirus Free** und wählen Sie **Deinstallieren**.
       d. Klicken Sie im angezeigten Fenster auf **NEU INSTALLIEREN**.

e. Warten Sie, bis die Neuinstallation abgeschlossen ist und starten Sie Ihr System neu.

- In **Windows 10**:

a. Klicken Sie auf **Start** und danach auf Einstellungen.

b. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie danach auf **Installierte Anwendungen**.

c. Suchen Sie **Bitdefender Antivirus Free** und wählen Sie **Deinstallieren**.

d. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.

e. Klicken Sie im angezeigten Fenster auf **NEU INSTALLIEREN**.

f. Warten Sie, bis die Neuinstallation abgeschlossen ist und starten Sie Ihr System neu.

Beachten Sie
Wenn Sie bei der Neuinstallation wie hier beschrieben vorgehen, werden Ihre benutzerdefinierte Einstellungen gespeichert und sind im neu installierten Produkt wieder verfügbar. Weitere Einstellungen werden unter Umständen wieder auf die Standardkonfiguration zurückgesetzt.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“ (S. 106)* beschrieben.

14.3. Ich kann eine App nicht mehr verwenden

Dieses Problem tritt auf, wenn Sie versuchen, ein Programm zu verwenden, das vor der Installation von Bitdefender einwandfrei funktioniert hatte.

Nach der Installation von Bitdefender könnten folgende Situationen eintreten:

- Sie könnten einen Benachrichtigung von Bitdefender erhalten, dass das Programm versucht, Veränderungen am System durchzuführen.
- Es ist möglich, dass Sie von dem Programm, das Sie starten möchten, eine Fehlermeldung erhalten.

Diese Situation tritt ein, wenn die Erweiterte Gefahrenabwehr eine Anwendung fälschlicherweise als Malware einstuft.

Die Erweiterte Gefahrenabwehr ist ein Bitdefender-Modul, das alle laufenden Anwendungen auf Ihren Systemen durchgehend überwacht und einen Bericht über jene sendet, die sich potenziell gefährlich verhalten. Da diese Funktion auf einem heuristischen System basiert, kann es dazu kommen, dass auch seriöse Anwendungen im Bericht der Erweiterten Gefahrenabwehr aufgelistet werden.

In solchen Fällen können Sie die entsprechende Anwendung von der Überwachung durch die Erweiterte Gefahrenabwehr ausnehmen.

So können Sie das Programm zur Ausnahmeliste hinzufügen:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Klicken Sie im Bereich **ADVANCED THREAT DEFENSE** auf **Öffnen**.
3. Klicken Sie im Fenster **Einstellungen** auf **Ausnahmen verwalten**.
4. Klicken Sie auf **+Ausnahme hinzufügen**.
5. Geben Sie den Pfad der ausführbaren Datei, die Sie vom Scan ausnehmen möchten, in das entsprechende Feld ein.

   Alternativ können Sie zu der ausführbaren Datei navigieren, indem Sie rechts in der Benutzeroberfläche auf die Schaltfläche "Durchsuchen" klicken, sie auswählen und dann auf **OK** klicken.
6. Aktivieren Sie den Schalter neben **Erweiterte Gefahrenabwehr**.
7. Klicken Sie auf **Speichern**.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“ (S. 106)* beschrieben.

14.4. Was können Sie tun, wenn Bitdefender eigentlich sichere Websites, Domains, IP-Adressen oder Online-Anwendungen blockiert?

Bitdefender ermöglicht Ihnen sicheres Surfen im Netz, indem es den Internet-Datenverkehr filtert und schädliche Inhalte blockiert. Es kann jedoch auch vorkommen, dass Bitdefender eigentlich sichere Websites, Domains, IP-Adressen oder Online-Anwendungen als unsicher einstuft, wodurch diese dann durch den Bitdefender-Scan des HTTP-Datenverkehrs irrtümlich blockiert werden.

Sollte die gleiche Seite, Domain, IP-Adresse oder Online-Anwendung wiederholt blockiert werden, können Sie diese zu den Ausnahmen hinzufügen, damit sie von den Bitdefender-Engines nicht mehr gescannt werden. So können Sie ungestört im Internet surfen.

So können Sie eine Website zu den **Ausnahmen** hinzufügen:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Klicken Sie im Bereich **ONLINE-GEFAHRENABWEHR** auf **Einstellungen**.
3. Klicken Sie auf **Ausnahmen verwalten**.
4. Klicken Sie auf **+Ausnahme hinzufügen**.
5. Geben Sie in das entsprechende Feld den Namen der Website, den Namen der Domain oder die IP-Adresse ein, die Sie zu den Ausnahmen hinzufügen möchten.
6. Klicken Sie auf den Schalter neben **Online-Gefahrenabwehr**.
7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Fenster zu schließen.

Nur Websites, Domains, IP-Adressen und Anwendungen, denen Sie uneingeschränkt vertrauen, sollten dieser Liste hinzugefügt werden. Diese werden dann von den folgenden Engines vom Scan ausgenommen: Bedrohung, Phishing und Betrug.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“ (S. 106)* beschrieben.

14.5. Wie man Bitdefender-Updates auch mit einer langsamen Internet-Verbindung durchführen kann

Falls Sie über eine langsame Internet-Verbindung (wie z. B. ein Modem) verfügen, können während des Updates Fehler auftreten.

So stellen Sie sicher, dass die Datenbank mit den Bedrohungsinformationen in Bitdefender jederzeit auf dem neuesten Stand ist:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Einstellungen**.
2. Wechseln Sie zum Reiter **Update**.
3. Deaktivieren Sie den Schalter **Update im Hintergrund**.

4. Beim nächsten Update werden Sie aufgefordert, das Update auszuwählen, das Sie herunterladen möchten. Wählen Sie nur **Virensignatur-Update**.
5. Bitdefender wird nur die Datenbank mit den Bedrohungsinformationen herunterladen und installieren.

14.6. Bitdefender-Dienste antworten nicht

Dieser Artikel hilft Ihnen bei der Lösung des Problems **Bitdefender-Dienste antworten nicht**. Sie könnten folgende Fehlermeldung erhalten:

- Das Bitdefender-Symbol im der Task-Leiste ist grau hinterlegt und Sie erhalten eine Meldung, dass die Bitdefender-Dienste nicht reagieren.
- Das Bitdefender-Fenster zeigt an, dass die Bitdefender-Dienste nicht antworten.

Der Fehler kann durch einen der folgenden Umstände verursacht werden:

- Temporäre Kommunikationsstörungen zwischen den Bitdefender-Diensten.
- Einige der Bitdefender-Dienste wurden angehalten.
- andere Sicherheitslösungen werden gleichzeitig mit Bitdefender auf Ihrem Gerät ausgeführt.

Um diesen Fehler zu beheben, versuchen Sie folgenden Lösungen:

1. Warten Sie einen Moment und beobachten Sie, ob sich etwas ändert. Der Fehler könnte vorübergehend sein.
2. Starten Sie das Gerät neu und warten Sie einige Momente, bis Bitdefender geladen ist. Öffnen Sie Bitdefender und überprüffen Sie ob das Problem immernoch besteht. Durch einen Neustart des Geräts wird das Problem üblicherweise behoben.
3. Überprüfen Sie, ob Sie irgendeine andere Sicherheitslösung installiert haben, weil diese den Normalbetrieb von Bitdefender stören könnte. Wenn dies der Fall ist, empfehlen wir Ihnen alle anderen Sicherheitslösungen zu entfernen und Bitdefender wieder neu zu installieren.

   Weitere Informationen finden Sie im Kapitel *„Wie entferne ich andere Sicherheitslösungen?“ (S. 56)*.

Sollte der Fehler weiterhin auftreten, wenden Sie sich bitte an unsere Support-Mitarbeiter, wie in Abschnitt *„Hilfe anfordern“ (S. 106)* beschrieben.

14.7. Entfernen von Bitdefender ist fehlgeschlagen

Wenn Sie Ihr Bitdefender-Produkt deinstallieren möchten und Sie bemerken, dass der Prozess hängen bleibt oder das System einfriert, klicken Sie auf **Abbrechen**. Sollte dies nicht zum Erfolg führen, starten Sie den Computer neu.

Falls die Deinstallation fehlschlägt, bleiben unter Umständen einige Bitdefender-Registry-Schlüssel und Dateien in Ihrem System. Solche Überbleibsel können eine erneute Installation von Bitdefender verhindern. Ebenso kann die Systemleistung und Stabilität leiden.

So können Sie Bitdefender vollständig von Ihrem System entfernen:

- In **Windows 7**:
  1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
  2. Suchen Sie **Bitdefender Antivirus Free** und wählen Sie **Deinstallieren**.
  3. Klicken Sie im angezeigten Fenster auf **Entfernen**.
  4. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.
- In **Windows 8 und Windows 8.1**:
  1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
  2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
  3. Suchen Sie **Bitdefender Antivirus Free** und wählen Sie **Deinstallieren**.
  4. Klicken Sie im angezeigten Fenster auf **Entfernen**.
  5. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.
- In **Windows 10**:
  1. Klicken Sie auf **Start** und danach auf Einstellungen.
  2. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie danach auf **Installierte Anwendungen**.
  3. Suchen Sie **Bitdefender Antivirus Free** und wählen Sie **Deinstallieren**.

4. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.
5. Klicken Sie im angezeigten Fenster auf **Entfernen**.
6. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.

14.8. Mein System fährt nach der Installation von Bitdefender nicht mehr hoch

Wenn Sie Bitdefender gerade installiert haben und Ihr System nicht mehr im Normalmodus starten können, kann es verschiedene Ursachen für dieses Problem geben.

Höchstwahrscheinlich wird es durch eine vorherige Bitdefender-Installation hervorgerufen, die nicht vollständig entfernt wurde. Eine weitere Möglichkeit ist eine andere Sicherheitslösung, die noch auf dem System installiert ist.

Im Folgenden finden Sie Herangehensweisen für die verschiedenen Situationen:

- **Sie hatten Bitdefender schon einmal im Einsatz und danach nicht vollständig von Ihrem System entfernt.**

  So können Sie das Problem lösen:

  1. Starten Sie Ihren Computer im abgesicherten Modus neu. Eine Anleitung hierzu finden Sie im Kapitel *„Wie führe ich einen Neustart im abgesicherten Modus durch?“* (S. 57).
  2. Entfernen Sie Bitdefender von Ihrem System:
     - In **Windows 7**:
       a. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.
       b. Suchen Sie **Bitdefender Antivirus Free** und wählen Sie **Deinstallieren**.
       c. Klicken Sie im angezeigten Fenster auf **Entfernen**.
       d. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.
       e. Starten Sie Ihren Computer im Normalmodus neu.
     - In **Windows 8 und Windows 8.1**:

a. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.

b. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.

c. Suchen Sie **Bitdefender Antivirus Free** und wählen Sie **Deinstallieren**.

d. Klicken Sie im angezeigten Fenster auf **Entfernen**.

e. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.

f. Starten Sie Ihren Computer im Normalmodus neu.

- In **Windows 10**:

a. Klicken Sie auf **Start** und danach auf Einstellungen.

b. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie danach auf **Installierte Anwendungen**.

c. Suchen Sie **Bitdefender Antivirus Free** und wählen Sie **Deinstallieren**.

d. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.

e. Klicken Sie im angezeigten Fenster auf **Entfernen**.

f. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.

g. Starten Sie Ihren Computer im Normalmodus neu.

3. Installieren Sie Ihr Bitdefender-Produkt erneut.

- **Sie hatten zuvor eine andere Sicherheitslösung im Einsatz und haben diese nicht vollständig entfernt.**

So können Sie das Problem lösen:

1. Starten Sie Ihren Computer im abgesicherten Modus neu. Eine Anleitung hierzu finden Sie im Kapitel *„Wie führe ich einen Neustart im abgesicherten Modus durch?“* (S. 57).
2. Entfernen Sie die andere Sicherheitslösung von Ihrem System:

- In **Windows 7**:

a. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme und Funktionen**.

b. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.

c. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.

- In **Windows 8 und Windows 8.1**:

  a. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.

  b. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.

  c. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.

  d. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.

- In **Windows 10**:

  a. Klicken Sie auf **Start** und danach auf Einstellungen.

  b. Klicken Sie im Bereich Einstellungen auf das **System**-Symbol und wählen Sie danach auf **Installierte Anwendungen**.

  c. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.

  d. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.

  Um die andere Software vollständig zu deinstallieren, rufen Sie die Hersteller-Website auf und führen Sie das entsprechende Deinstallations-Tool aus oder wenden Sie sich direkt an den Hersteller, um eine Deinstallationsanleitung zu erhalten.

3. Starten Sie Ihr System im Normalmodus neu und installieren Sie Bitdefender erneut.

Sie haben die oben beschriebenen Schritte bereits durchgeführt und das Problem besteht weiterhin.

So können Sie das Problem lösen:

1. Starten Sie Ihren Computer im abgesicherten Modus neu. Eine Anleitung hierzu finden Sie im Kapitel *„Wie führe ich einen Neustart im abgesicherten Modus durch?“* (S. 57).
2. Nutzen Sie die Systemwiederherstellung von Windows, um das Gerät zu einem früheren Zeitpunkt wiederherzustellen, bevor das Bitdefender-Produkt installiert wurde.
3. Starten Sie das System im Normalmodus neu und wenden Sie sich an unsere Support-Mitarbeiter, wie in Abschnitt *„Hilfe anfordern“* (S. 106) beschrieben.

15. ENTFERNUNG VON BEDROHUNGEN

Bedrohungen können Ihr System auf vielfältige Art und Weise beeinträchtigen. Wie Bitdefender auf diese Malware darauf reagiert, hängt von der Art der Bedrohung ab. Da Bedrohungen ihr Verhalten ständig ändern, ist es schwierig ein Muster für ihr Verhalten und ihre Aktionen festzulegen.

Es gibt Situationen, in denen Bitdefender eine Bedrohung Ihres Systems nicht automatisch entfernen kann. In solch einem Fall ist Ihre Intervention nötig.

- ???
- *„Was ist zu tun, wenn Bitdefender Bedrohungen auf Ihrem Gerät findet?“* (S. 98)
- *„Wie entferne ich eine Bedrohung aus einem Archiv?“* (S. 100)
- *„Wie entferne ich eine Bedrohung aus einem E-Mail-Archiv?“* (S. 101)
- *„Wie gehe ich vor, wenn ich eine Datei für gefährlich halte?“* (S. 102)
- *„Wobei handelt es sich bei den passwortgeschützten Dateien im Scan-Protokoll?“* (S. 103)
- *„Wobei handelt es sich bei den übersprungenen Objekten im Scan-Protokoll?“* (S. 103)
- *„Wobei handelt es sich bei den zu stark komprimierten Dateien im Scan-Protokoll?“* (S. 103)
- *„Warum hat Bitdefender ein infizierte Datei automatisch gelöscht?“* (S. 104)

Wenn Sie Ihr Problem hier nicht finden oder wenn die vorgeschlagene Lösung nicht zum Erfolg führt, können Sie den technischen Kundendienst von Bitdefender wie in Kapitel *„Hilfe anfordern“* (S. 106) beschrieben, kontaktieren.

15.1. Was ist zu tun, wenn Bitdefender Bedrohungen auf Ihrem Gerät findet?

Es gibt verschiedene Möglichkeiten, wie Sie von einer Bedrohung auf Ihrem Gerät erfahren:

- Sie haben einen Scan Ihres Geräts durchgeführt und Bitdefender hat infizierte Objekte gefunden.

- Eine Bedrohungswarnung informiert Sie, dass Bitdefender einen oder mehrere Bedrohungen auf Ihrem Gerät blockiert hat.

In solchen Situationen sollten Sie Bitdefender aktualisieren, um sicherzustellen, dass Sie über die neuesten Bedrohungsinformationen verfügen und einen System-Scan durchführen, um das System zu prüfen.

Sobald der System-Scan abgeschlossen ist, wählen Sie die gewünschte Aktion für die infizierten Objekte aus (Desinfizieren, Löschen, In Quarantäne verschieben).

Warnung

Wenn Sie den Verdacht haben, dass die Datei Teil des Windows-Betriebssystems ist oder dass es sich nicht um eine infizierte Datei handelt, folgen Sie NICHT diesen Schritten und kontaktieren Sie so bald wie möglich den Bitdefender-Kundendienst.

Falls die ausgewählte Aktion nicht durchgeführt werden konnte und im Scan-Protokoll ersichtlich ist, dass Ihr PC mit einer Bedrohung infiziert ist, die nicht gelöscht werden kann, müssen Sie die Datei(en) manuell entfernen.

Die erste Methode kann im Normalmodus eingesetzt werden:

1. Deaktivieren Sie den Bitdefender-Echtzeitvirenschutz:
   a. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
   b. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Öffnen**.
   c. Deaktivieren Sie im Fenster **Erweitert** die Option **Bitdefender-Schild**.
2. Lassen Sie sich die verborgenen Objekte in Windows anzeigen. Eine Anleitung hierzu finden Sie im Kapitel *„Wie kann ich in Windows versteckte Objekte anzeigen?“* (S. 55).
3. Blättern Sie zum Laufwerk, in dem die infizierte Datei gespeichert ist (siehe Scan-Protokoll) und löschen Sie sie.
4. Aktivieren Sie den Bitdefender-Echtzeitvirenschutz.

Falls die Infektion mit der ersten Methode nicht entfernt werden konnte:

1. Starten Sie Ihren Computer im abgesicherten Modus neu. Eine Anleitung hierzu finden Sie im Kapitel *„Wie führe ich einen Neustart im abgesicherten Modus durch?“* (S. 57).

2. Lassen Sie sich die verborgenen Objekte in Windows anzeigen. Eine Anleitung hierzu finden Sie im Kapitel *„Wie kann ich in Windows versteckte Objekte anzeigen?“ (S. 55)*.
3. Blättern Sie zum Laufwerk, in dem die infizierte Datei gespeichert ist (siehe Scan-Protokoll) und löschen Sie sie.
4. Starten Sie Ihren Computer neu und starten Sie den Normalmodus.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“ (S. 106)* beschrieben.

15.2. Wie entferne ich eine Bedrohung aus einem Archiv?

Bei einem Archiv handelt es sich um eine Datei oder eine Dateisammlung, die mit einem speziellen Format komprimiert wurde, um so den benötigten Festplattenplatz zu reduzieren.

Einige dieser Formate sind offene Formate und bieten Bitdefender die Möglichkeit, diese zu scannen und die entsprechenden Aktionen durchzuführen, um sie zu entfernen.

Andere Archivformate sind teilweise oder komplett geschlossen und Bitdefender kann nur das Vorhandensein von Bedrohungen innerhalb dieser Archive feststellen, nicht jedoch andere Aktionen ausführen.

Wenn Bitdefender Sie darüber informiert, dass eine Bedrohung innerhalb eines Archivs gefunden wurde und keine Aktion verfügbar ist, bedeutet dies, dass die Bedrohung aufgrund möglicher Restriktionen der Zugriffseinstellungen des Archivs nicht entfernt werden kann.

So können Sie eine in einem Archiv gespeicherte Bedrohung entfernen.

1. Führen Sie einen System-Scan durch, um das Archiv zu finden, in dem sich die Bedrohung befindet.
2. Deaktivieren Sie den Bitdefender-Echtzeitvirenschutz:
   a. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
   b. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Öffnen**.
   c. Deaktivieren Sie im Fenster **Erweitert** die Option **Bitdefender-Schild**.

3. Gehen Sie zum Speicherort des Archivs und dekomprimieren Sie es mit einem Archivierungsprogramm wie beispielsweise WinZip.
4. Identifizieren Sie die infizierte Datei und löschen Sie sie.
5. Löschen Sie das Originalarchiv, um sicherzugehen, dass die Infizierung vollständig entfernt ist.
6. Komprimieren Sie die Dateien erneut in einem neuen Verzeichnis und verwenden Sie dafür ein Komprimierprogramm wie WinZip.
7. Aktivieren Sie den Bitdefender-Echtzeit-Virenschutz und führen Sie einen System-Scan durch, um so sicherzustellen, dass Ihr System nicht anderweitig infiziert ist.

Beachten Sie

Es ist wichtig zu beachten, dass eine in einem Archiv gespeicherte Bedrohung für Ihr System keine unmittelbare Bedrohung darstellt, da die Bedrohung dekomprimiert und ausgeführt werden muss, bevor sie Ihr System infizieren kann.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“ (S. 106)* beschrieben.

15.3. Wie entferne ich eine Bedrohung aus einem E-Mail-Archiv?

Bitdefender kann auch Bedrohungen in E-Mail-Datenbanken und auf Festplatten gespeicherten E-Mail-Archiven aufspüren.

Manchmal ist es notwendig, die infizierte Nachricht über die im Scan-Bericht zur Verfügung gestellten Informationen zu identifizieren und sie dann manuell zu löschen.

So können Sie in einem E-Mail-Archiv gespeicherte Bedrohungen entfernen:

1. Scannen Sie die E-Mail-Datenbank mit Bitdefender.
2. Deaktivieren Sie den Bitdefender-Echtzeitvirenschutz:
   a. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
   b. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Öffnen**.
   c. Deaktivieren Sie im Fenster **Erweitert** die Option **Bitdefender-Schild**.

3. Öffnen Sie den Scan-Bericht und nutzen Sie die Identifikationsinformation (Betreff, Von, An) der infizierten Nachricht, um den dazugehörigen E-Mail-Client zu finden.
4. Löschen Sie die infizierte Nachricht. Die meisten E-Mail-Clients verschieben gelöschte Nachrichten in ein Wiederherstellungsordner, von dem aus sie wiederhergestellt werden können. Sie sollten sicherstellen, dass die Nachricht auch aus diesem Recovery-Verzeichnis gelöscht ist.
5. Komprimieren Sie das Verzeichnis, in dem die infizierte Nachricht gespeichert wird.
   - In Microsoft Outlook 2007: Klicken Sie im Dateimenü auf "Datendateiverwaltung". Wählen Sie das persönliche Verzeichnis (.pst), das Sie komprimieren möchten und klicken Sie auf "Einstellungen". Klicken Sie auf Jetzt komprimieren.
   - In Microsoft Outlook 2010 / 2013/ 2016: Klicken Sie im Dateimenü auf Info und dann Kontoeinstellungen (Konten hinzufügen oder entfernen bzw. vorhandene Verbindungseinstellungen ändern). Klicken Sie danach auf Datendatei, markieren Sie die persönlichen Ordner-Dateien (.pst), die Sie komprimieren wollen, und klicken Sie auf Einstellungen. Klicken Sie auf Jetzt komprimieren.
6. Aktivieren Sie den Bitdefender-Echtzeitvirenschutz.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“ (S. 106)* beschrieben.

15.4. Wie gehe ich vor, wenn ich eine Datei für gefährlich halte?

Möglicherweise halten Sie eine Datei auf Ihrem System für gefährlich, obwohl Ihr Bitdefender-Produkt keine Gefahr erkannt hat.

So können Sie sicherstellen, dass Ihr System geschützt ist:

1. Führen Sie einen **System-Scan** mit Bitdefender durch. Eine Anleitung hierzu finden Sie im Kapitel *„Wie scanne ich mein System?“ (S. 43)*.
2. Wenn der Scan ein sauberes Ergebnis liefert, Sie aber weiterhin Zweifel an der Sicherheit der Datei hegen und ganz sicher gehen möchten, wenden Sie sich bitte an unsere Support-Mitarbeiter, damit wir Ihnen helfen können.

   Eine Anleitung hierzu finden Sie im Kapitel *„Hilfe anfordern“ (S. 106)*.

15.5. Wobei handelt es sich bei den passwortgeschützten Dateien im Scan-Protokoll?

Dies ist nur eine Benachrichtigung, dass die von Bitdefender gefundenen Dateien entweder passwortgeschützt oder anderweitig verschlüsselt sind.

Am häufigsten sind passwortgeschützte Objekte:

- Dateien, die zu einer anderen Sicherheitslösung gehören.
- Dateien, die zum Betriebssystem gehören.

Um die Inhalte tatsächlich zu scannen, müssen diese Dateien entweder extrahiert oder anderweitig entschlüsselt werden.

Sollten diese Inhalte extrahiert werden, wird der Echtzeit-Scanner von Bitdefender diese automatisch scannen, um so den Schutz Ihres Geräts zu gewährleisten. Wenn Sie diese Dateien mit Bitdefender scannen möchten, müssen Sie den Produkthersteller kontaktieren, um nähere Details zu diesen Dateien zu erhalten.

Unsere Empfehlung ist, diese Dateien zu ignorieren, da Sie für Ihr System keine Bedrohung darstellen.

15.6. Wobei handelt es sich bei den übersprungenen Objekten im Scan-Protokoll?

Alle Dateien, die im Scan-Protokoll als "Übersprungen" ausgewiesen werden, sind sauber.

Für eine bessere Leistung scannt Bitdefender keine Dateien, die seit dem letzten Scan nicht verändert wurden.

15.7. Wobei handelt es sich bei den zu stark komprimierten Dateien im Scan-Protokoll?

Die zu stark komprimierten Objekte sind Elemente, die durch die Scan-Engine nicht extrahiert werden konnten oder Elemente, für die eine Entschlüsselung zu viel Zeit in Anspruch genommen hätte und die dadurch das System instabil machen würden.

Überkomprimiert bedeutet, dass Bitdefender das Scannen von Archiven übersprungen hat, da das Entpacken dieser zu viele Systemressourcen in Anspruch genommen hätte. Der Inhalt wird, wenn nötig, in Echtzeit gescannt.

15.8. Warum hat Bitdefender ein infizierte Datei automatisch gelöscht?

Wird eine infizierte Datei gefunden, versucht Bitdefender automatisch, diese zu desinfizieren. Falls die Desinfizierung fehlschlägt, wird die Datei in die Quarantäne verschoben, um dort die Infizierung einzudämmen.

Bestimmte Bedrohungsarten können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

Dies geschieht normalerweise bei Installationsdateien, die von nicht vertrauenswürdigen Seiten heruntergeladen werden. Wenn Sie auf ein solches Problem stoßen, laden Sie die Installationsdatei von der Website des Herstellers oder einer anderen vertrauenswürdigen Website herunter.

KONTAKTIEREN SIE UNS

16. HILFE ANFORDERN

Bitdefender bietet seinen Kunden konkurrenzlos schnellen und kompetenten Support. Sollten sich Probleme ergeben oder Sie eine Frage zu Ihrem Bitdefender-Produkt haben, so stehen Ihnen verschiedene Online-Quellen zur Verfügung, wo Sie Lösungen und Antworten finden. Sie können sich auch jederzeit an den Bitdefender-Kundendienst wenden. Unsere Kundenbetreuer beantworten Ihre Fragen zügig und bieten Ihnen die benötigte Unterstützung.

Im Abschnitt *„Verbreitete Probleme beheben“* (S. 85) finden Sie alle wichtigen Informationen zu den häufigsten Problemen, die bei der Verwendung dieses Produkts auftreten können.

Wenn Sie in den vorhandenen Quellen keine Antwort auf Ihre Frage finden, können Sie uns direkt kontaktieren:

- „Kontaktieren Sie uns direkt über die Bitdefender Antivirus Free-Oberfläche“ (S. 106)
- „Kontaktieren Sie uns über unser Online-Support-Center“ (S. 107)

Kontaktieren Sie uns direkt über die Bitdefender Antivirus Free-Oberfläche

Wenn Sie über eine aktive Internet-Verbindung verfügen, können Sie Bitdefender direkt aus der Benutzeroberfläche heraus kontaktieren, um Hilfe zu erhalten.

Folgen Sie diesen Schritten:

1. Klicken Sie auf die **Support**-Schaltfläche, dargestellt durch ein **Fragezeichen** im oberen Bereich der Bitdefender-Oberfläche.
2. Sie haben die folgenden Möglichkeiten:
   - **BENUTZERHANDBUCH**

     Hier können Sie unsere Datenbank nach den gewünschten Informationen durchsuchen.
   - **SUPPORT-CENTER**

     Greifen Sie auf unsere Online-Artikel und Videoanleitungen zu.
   - **ASK THE COMMUNITY**

Click **ASK THE COMMUNITY** to access the Bitdefender community where you can get answers and guidance from other Bitdefender users.

Kontaktieren Sie uns über unser Online-Support-Center

Wenn Sie über das Bitdefender-Produkt nicht auf die notwendigen Informationen zugreifen können, wenden Sie sich bitte an unser Online-Support-Center.

1. Gehen Sie zu https://www.bitdefender.de/support/consumer.html.

   Im Bitdefender-Support-Center finden Sie eine Vielzahl von Beiträgen, die Lösungen zu Problemen im Zusammenhang mit Bitdefender bereithalten.

2. Nutzen Sie die Suchleiste oben im Fenster, um Artikel zu finden, die eine Lösung für Ihr Problem enthalten könnten. Geben Sie dazu einen Begriff in die Suchleiste ein und klicken Sie auf **Suchen**.

3. Lesen Sie die relevanten Artikel oder Dokumente und probieren Sie die vorgeschlagenen Lösungen aus.

4. Wenn die dort vorgeschlagene Lösung das Problem nicht behebt, gehen Sie zu

   http://www.bitdefender.de/support/contact-us.htmlund kontaktieren Sie unseren Kundendienst.

17. ONLINE-RESSOURCEN

Für die Lösung Ihres Problems und Fragen im Zusammenhang mit Bitdefender stehen Ihnen verschiedene Online-Ressourcen zur Verfügung.

- Bitdefender-Support-Center:

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

- Bitdefender Support-Forum:

  https://forum.bitdefender.com

- Das Computer-Sicherheitsportal HOTforSecurity:

  https://www.hotforsecurity.com

Zudem können Sie auch Ihre favorisierte Suchmaschine nutzen, um mehr zu erfahren über Computersicherheit, die Bitdefender-Produkte und das Unternehmen.

17.1. 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.

Das Bitdefender-Support-Center ist öffentlich zugänglich und frei durchsuchbar. Die darin enthaltenen Informationen sind äußerst umfangreich und stellen eine weitere Methode dar, mit der Bitdefender-Kunden mit dem notwendigen technischen Wissen versorgt werden. 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 steht Ihnen jederzeit unter der folgenden Adresse zur Verfügung:

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

17.2. Bitdefender Support-Forum

Das Bitdefender Support-Forum bietet Bitdefender-Anwendern eine Möglichkeit, Hilfe zu erhalten oder anderen Hilfestellung zu geben.

Falls Ihr Bitdefender-Produkt nicht richtig funktioniert, bestimmte Bedrohungen nicht von Ihrem Gerät entfernen kann oder wenn Sie Fragen über die Funktionsweise haben, stellen Sie Ihr Problem oder Frage in das Forum ein.

Support-Techniker von Bitdefender überwachen neue Einträge in das Forum, um Ihnen helfen zu können. Außerdem können Sie eine Antwort auf Ihre Frage oder einen Lösungsvorschlag von einem bereits erfahrenen Bitdefender-Anwender erhalten.

Bevor Sie einen Eintrag ins Forum stellen, suchen Sie im Forum nach einem ähnlichen oder verwandten Themenbereich.

Das Bitdefender Support-Forum finden Sie unter https://forum.bitdefender.com. Es steht in 5 verschiedenen Sprachen zur Verfügung: Englisch, Deutsch, Französisch, Spanisch und Rumänisch. Für den Zugriff auf den Bereich Konsumgüter klicken Sie bitte auf **Schutz für Privatanwender**.

17.3. Das Portal HOTforSecurity

HOTforSecurity bietet umfangreiche Informationen rund um das Thema Computer-Sicherheit. Hier erfahren Sie mehr über die verschiedenen Bedrohungen, denen Ihr Gerät während einer bestehenden Internetverbindung ausgesetzt ist (Malware, Phishing, Spams, Cyber-Kriminelle).

Ständig werden neue Artikel zu den neuesten Threats, aktuellen Sicherheitstrends und anderen Informationen zur Computersicherheits-Branche eingestellt, damit Sie up-to-date bleiben.

Die Adresse von HOTforSecurity ist https://www.hotforsecurity.com.

18. KONTAKTINFORMATIONEN

Effiziente Kommunikation ist der Schlüssel zu einem erfolgreichen Unternehmen. BITDEFENDER hat sich seit 2001 einen herausragenden Ruf erarbeitet, indem es seine Kommunikation immer besser gemacht hat, um die Erwartungen unserer Kunden und Partner noch zu übertreffen. Für jedwede Fragen stehen wir Ihnen gerne zur Verfügung.

18.1. Kontaktadressen

Vertrieb: vertrieb@bitdefender.de
Support-Center:https://www.bitdefender.de/support/consumer.html
Dokumentation: documentation@bitdefender.com
Händler vor Ort:https://www.bitdefender.de/partners/
Partnerprogramm: partners@bitdefender.com
Medienkontakt: pr@bitdefender.com
Karriere: jobs@bitdefender.com
Bedrohungseinsendungen: virus_submission@bitdefender.com
Spam-Einsendungen: spam_submission@bitdefender.com
Missbrauch melden: abuse@bitdefender.com
Webseite:https://www.bitdefender.de

18.2. Lokale Vertriebspartner

Bitdefender-Händler stehen für vertriebliche und allgemeine Fragen und Informationen in ihren jeweiligen Regionen jederzeit zur Verfügung.

So finden Sie einen Bitdefender-Händler in Ihrem Land:

1. Gehen Sie zu http://www.bitdefender.de/partners/partner-locator.html.
2. Geben Sie über die entsprechenden Optionen Ihren Wohnort und Ihr Land an.
3. Falls Sie in Ihrem Land keinen Bitdefender-Händler finden, können Sie uns gerne unter vertrieb@bitdefender.de kontaktieren. Schreiben Sie uns Ihre E-Mail in Englisch, damit wir Ihnen umgehend helfen können.

18.3. Bitdefender-Niederlassungen

Bitdefender-Niederlassungen stehen Ihnen für betriebliche und allgemeine Fragen und Informationen in ihren jeweiligen Bereichen jederzeit zur

Verfügung. Die genauen Kontaktdaten und Adressen finden Sie in der unten stehenden Auflistung.

U.S.A

Bitdefender, LLC
6301 NW 5th Way, Suite 4300
Fort Lauderdale, Florida 33309
Telefon (Geschäftsstelle&Vertrieb): 1-954-776-6262
Vertrieb: sales@bitdefender.com
Technischer Support: https://www.bitdefender.com/support/consumer.html
Web: https://www.bitdefender.com

Großbritannien und Irland

BITDEFENDER LTD
C/O Howsons Winton House, Stoke Road, Stoke on Trent
Staffordshire, United Kindon, ST4 2RW
E-Mail: info@bitdefender.co.uk
Telefon: (+44) 2036 080 456
Vertrieb: sales@bitdefender.co.uk
Technischer Support: https://www.bitdefender.co.uk/support/
Web: https://www.bitdefender.co.uk

Deutschland

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Geschäftsstelle: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Vertrieb: vertrieb@bitdefender.de
Technischer Support: https://www.bitdefender.de/support/consumer.html
Web: https://www.bitdefender.de

Dänemark

Bitdefender APS
Agern Alle 24, 2970 Hørsholm, Denmark
Geschäftsstelle: +45 7020 2282

Technischer Support: http://bitdefender-antivirus.dk/
Web: http://bitdefender-antivirus.dk/

Spanien

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Telefon: +34 902 19 07 65
Vertrieb: comercial@bitdefender.es
Technischer Support: https://www.bitdefender.es/support/consumer.html
Webseite: https://www.bitdefender.es

Rumänien

BITDEFENDER SRL
Orhideea Towers Building, 15A Orhideelor Street, 11th fllor, district 6
Bucharest
Fax: +40 21 2641799
Telefon Vertrieb: +40 21 2063470
Vertrieb EMail: sales@bitdefender.ro
Technischer Support: https://www.bitdefender.ro/support/consumer.html
Webseite: https://www.bitdefender.ro

Vereinigte Arabische Emirate

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Telefon Vertrieb: 00971-4-4588935 / 00971-4-4589186
Vertrieb EMail: mena-sales@bitdefender.com
Technischer Support: https://www.bitdefender.com/support/consumer.html
Webseite: https://www.bitdefender.com

Glossar

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.

Advanced Persitent Threats

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.

AktiveX

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.

Aktivierungs-Code

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

Arbeitsspeicher

Interne Speicherbereiche im Rechner. Der Begriff Arbeitsspeicher bezeichnet Datenträger in Form von sehr schnellen Chips. Dies steht im Gegensatz zu Speicherplatz, der sich auf Magnetbändern oder Datenträgern befindet. Jeder Rechner hat eine gewisse Menge Arbeitsspeicher. Dieser wird auch Hauptspeicher oder RAM bezeichnet.

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.

Backdoor (Hintertür)

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

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.

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.

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.

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.

Cookie

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.

Dateierweiterung

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.

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.

Durchsuchen

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.

E-Mail

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

E-Mail Client

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

Ereignisanzeige

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

Exploits

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

Fehlalarm

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

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

Keylogger

Ein Keylogger ist eine Anwendung, die alle Ihre Tastenanschläge aufzeichnet.

Keylogger sind an sich nicht schädlich. Sie können auch legitim eingesetzt werden, um beispielsweise die Aktivitäten von Angestellten oder Kindern zu überwachen. Sie werden jedoch zunehmend von

Cyber-Kriminellen mit bösartiger Absicht eingesetzt (um beispielsweise private Daten wie Benutzernamen oder Passwörter zu sammeln).

Komprimierte Programme

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

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

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.

Logdatei (Berichtsdatei)

Eine Datei, die stattgefundene Aktivitäten aufzeichnet. Zum Beispiel speichert Bitdefender eine Prokolldatei mit den geprüften Pfaden, Ordnern, der Anzahl der gescannten Archive und Dateien sowie der Anzahl der gefundenen infizierten oder verdächtigen Dateien.

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.

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-Belästigung

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.

Pfad

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

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

Phishing

Das Senden einer E-Mail an einen Benutzer, in der der Sender sich als Vertreter eines legitimen Unternehmens ausgibt und versucht, den Empfänger so zu manipulieren, dass er persönliche Informationen preisgibt, die dann zum Diebstahl der Identität verwendet werden können. Die E-Mail leitet den Benutzer dann auf eine Webseite, auf der er aufgefordert wird, vertrauliche Daten wie Kreditkartennummern, TANs oder PINs preiszugeben. Es wird oft vorgegeben, dass dies aus Gründen der Aktualisierung geschehen soll. Diese Webseiten sind jedoch gefälscht und wurden eigens für den Diebstahl dieser Daten eingerichtet.

Photon

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

Polymorpher 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.

Ransomware

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

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

Rootkit

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

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

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

Schnittstelle

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

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

Script

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

Spam

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

Spyware

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

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

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

Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.

Startup Objekt (Autostart-Objekt)

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

Symbolleiste

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

TCP/IP

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

Trojaner

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

Der Begriff entstammt einer Geschichte in Homers "Ilias", in der die Griechen ihren Feinden, den Trojanern, angeblich als Sühnegabe ein riesiges hölzernes Pferd schenkten. Aber nachdem die Trojaner das Pferd in die Stadt gebracht hatten, schlichen sich die im Bauch des hölzernen Pferdes versteckten Soldaten bei Nacht heraus, öffneten die

Tore der Stadt und ermöglichten somit ihren Landsleuten, in die Stadt einzudringen und auf diese Weise Troja zu besetzen.

Update (Aktualisierung)

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

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

Update der Bedrohungsinformationen

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

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.

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.

Wurm

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