



Bitdefender®

**Bitdefender Endpoint
Security Tools für
Windows**

BENUTZERHANDBUCH

Bitdefender Endpoint Security Tools für Windows Benutzerhandbuch

Veröffentlicht 2019.11.29

Copyright© 2019 Bitdefender

Rechtlicher Hinweis

Alle Rechte vorbehalten. Bestandteile dieses Handbuchs dürfen weder in elektronischer noch mechanischer Form reproduziert werden. Dies gilt auch für das Fotokopieren, Aufnehmen oder jegliche andere Form von Datenspeicherung oder Informationsbeschaffung, ohne die Zustimmung von Bitdefender. Ausnahmen gelten für Zitate in Verbindung mit Testberichten. Der Inhalt darf in keiner Weise verändert werden.

Warnung und Haftungsausschluss. Dieses Produkt und die dazugehörige Dokumentation sind urheberrechtlich geschützt. Die Informationen in diesem Dokument werden „ohne Mängelgewähr“ gegeben. Obwohl dieses Dokument mit äußerster Sorgfalt erstellt und geprüft wurde, übernehmen die Autoren keinerlei Haftung für tatsächlich oder angeblich auftretende Schäden bzw. Datenverluste, die direkt oder indirekt durch die Informationen in diesem Dokument entstehen könnten oder bereits entstanden sind.

Dieses Handbuch enthält Verweise auf andere, nicht von Bitdefender erstellte oder von Bitdefender kontrollierte Webseiten und somit übernimmt Bitdefender auch keine Verantwortung für die Inhalte dieser Webseiten. Der Besuch der in diesem Dokument aufgelisteten Drittanbieter-Webseiten erfolgt damit auf eigene Gefahr. Bitdefender stellt diese Links der Einfachheit zur Verfügung. Dies bedeutet nicht, dass Bitdefender den Inhalt einer Website Dritter befürwortet oder Verantwortung dafür übernimmt.

Warenzeichen. Es erscheinen eingetragene Warenzeichen in diesem Dokument. Alle eingetragenen und nicht eingetragenen Warenzeichen in diesem Dokument sind das alleinige Eigentum der jeweiligen Besitzer.

Inhaltsverzeichnis

| | |
|--|----|
| Vorwort | iv |
| 1. Zielsetzung und Zielgruppe | iv |
| 2. Über dieses Handbuch | iv |
| 3. In diesem Handbuch verwendete Konventionen | iv |
| 4. Ihre Mithilfe | v |
| 1. Erste Schritte | 1 |
| 1.1. Das Task-Leisten-Symbol | 1 |
| 1.2. Das Hauptfenster | 2 |
| 1.2.1. Dem Statusbereich | 3 |
| 1.2.2. Ereignischronik | 4 |
| 1.3. Das Modulfenster | 5 |
| 1.4. Aktionsmenü | 11 |
| 2. Scannen auf Malware | 13 |
| 2.1. Scannen von Dateien und Ordnern | 13 |
| 2.2. Durchführen von Quick Scans | 13 |
| 2.3. Einen Vollständigen Scan ausführen | 14 |
| 2.4. Konfigurieren und Ausführen eines benutzerdefinierten Scans | 15 |
| 2.4.1. Dateitypen | 16 |
| 2.4.2. Was soll gescannt werden? | 17 |
| 2.4.3. Aktionen bei Fund | 18 |
| 2.5. Prüfen der Scan-Protokolle | 19 |
| 3. Verwendung der Laufwerksverschlüsselung | 21 |
| 3.1. Wie Sie Ihr System verschlüsseln | 21 |
| 3.2. Entschlüsselung Ihres Systems | 23 |
| 3.3. Überprüfung des Verschlüsselungsstatus | 23 |
| 3.4. Ändern der/des Verschlüsselungs-PIN/Passworts | 24 |
| 4. Aktualisierung | 25 |
| 4.1. Arten von Updates | 25 |
| 4.2. Überprüft, ob Ihr Schutz auf dem neuesten Stand ist | 26 |
| 4.3. Durchführung eines Updates | 26 |
| 5. Ereignisanzeige | 27 |
| 6. Verwenden der Befehlszeilenoberfläche | 29 |
| 6.1. Unterstützte Befehle | 30 |
| 6.2. Befehlszeilen-Fehlercodes | 39 |
| 7. Hilfe erhalten | 41 |
| Glossar | 42 |

Vorwort

1. Zielsetzung und Zielgruppe

Diese Dokumentation richtet sich an die Endanwender von **Bitdefender Endpoint Security Tools**, der Security for Endpoints-Client-Software, die auf Computern und Servern installiert wird, um diese vor Malware und anderen Bedrohungen aus dem Internet zu schützen und die Einhaltung von Richtlinien für die Benutzerkontrolle sicherzustellen.

Die hier bereitgestellten Informationen sollten für jeden Benutzer mit Erfahrung im Umgang mit Windows verständlich sein.

2. Über dieses Handbuch

Dieses Handbuch ist übersichtlich gestaltet, damit Sie im Handumdrehen alle benötigten Informationen finden können.

[„Erste Schritte“ \(S. 1\)](#)

Mit der Bitdefender Endpoint Security Tools-Benutzeroberfläche vertraut werden.

[„Scannen auf Malware“ \(S. 13\)](#)

Malware-Scans durchführen lernen.

[„Aktualisierung“ \(S. 25\)](#)

Mehr über Updates für Bitdefender Endpoint Security Tools erfahren.

[„Ereignisanzeige“ \(S. 27\)](#)

Die Aktivität von Bitdefender Endpoint Security Tools überprüfen.

[„Hilfe erhalten“ \(S. 41\)](#)

Beschreibt wie Sie Hilfe bzw. Unterstützung zu dem Produkt erhalten und erhält zusätzlich eine Liste mit den am häufigsten gestellten Fragen (FAQ).

3. In diesem Handbuch verwendete Konventionen


Typografie


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

| Erscheinungsbild | Beschreibung |
|--|--|
| business-docs@bitdefender.com | Verweise auf E-Mail-Adressen, z.B. zur Kontaktaufnahme. |
| „Vorwort“ (S. iv) | Interne Verweise (Links) auf beliebige Stellen innerhalb dieses Dokuments. |
| Dateiname | Dateien und Verzeichnisse werden in einer Schriftart mit fester Laufweite angegeben. |
| Option | Alle Produktoptionen werden fett gedruckt dargestellt. |
| Stichwort | Wichtige Stichwörter oder Begriffe werden durch Fettdruck hervorgehoben. |

Hinweise

Hierbei handelt es sich um Hinweise innerhalb des Textflusses, welche mit einer kleinen Grafik markiert sind. Es handelt sich um Informationen, die Sie in jedem Fall beachten sollten.

 **Beachten Sie**
Diese Bemerkung dient lediglich zur Überprüfung. Notizen enthalten in der Regel nützliche Informationen wie zum Beispiel einen Verweis auf ein verwandtes Thema.

 **Wichtig**
Diese Art von Hinweis sollte in jedem Fall gelesen werden. Es werden wichtige Informationen zum jeweiligen Thema gegeben, die nicht übersprungen werden sollten.

4. Ihre Mithilfe

Bitte teilen Sie uns mit, was Ihrer Meinung nach an diesem Leitfaden verbessert werden könnte, damit wir Ihnen die bestmögliche Dokumentation für Ihre Software bieten können.

Falls Sie dennoch Fehler finden, so teilen Sie uns diese bitte mit indem Sie uns per E-Mail unter der Adresse business-docs@bitdefender.com kontaktieren.

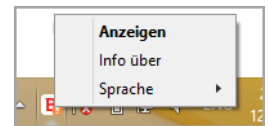
1. ERSTE SCHRITTE

Bitdefender Endpoint Security Tools ist ein vollautomatisches Computer-Sicherheitsprogramm, das von Ihrem Netzwerkadministrator fernverwaltet wird. Nach der Installation schützt sie Sie vor allen Arten von Schad-Software (wie Viren, Spyware und Trojaner), Netzwerkangriffen, Phishing-Versuchen und Datendiebstahl. Es kann zudem eingesetzt werden, um die Einhaltung von Richtlinien zur Computer- und Internetnutzung in Ihrem Unternehmen durchzusetzen. Bitdefender Endpoint Security Tools trifft sicherheitsrelevante Entscheidungen autonom und zeigt dabei nur sehr selten Sicherheitsmeldungen an. Details zu den durchgeführten Aktionen und Informationen zum Betrieb des Programms erhalten Sie in der **Ereignisse**-Zeitleiste.

1.1. Das Task-Leisten-Symbol

Nach der Installation wird ein Bitdefender Endpoint Security Tools-Symbol **B** dauerhaft in Ihrer Task-Leiste angezeigt. Bei einem Doppelklick auf dieses Symbol öffnet sich das Hauptfenster. Mit einem Rechtsklick auf das Symbol öffnen Sie ein Kontextmenü mit nützlichen Optionen.

- **Anzeigen** - Öffnet das Bitdefender Endpoint Security Tools-Hauptfenster.
- **Über** - öffnet ein Fenster mit Informationen über Bitdefender Endpoint Security Tools und hilft Ihnen dabei Antworten zu finden, falls einmal Probleme auftreten. In diesem Fenster finden Sie auch einen Link zur Bitdefender-Datenschutzerklärung.
- **Sprache** - hier können Sie die Sprache der Benutzeroberfläche einstellen.
- **Power-User** - hierüber können Sie Sicherheitseinstellungen verändern, nachdem Sie im Anmeldefenster das entsprechende Passwort eingegeben haben. Im Control Center wird eine Benachrichtigung angezeigt, wenn ein Endpunkt sich im Power-User-Modus befindet, und Control Center-Administratoren können lokale Sicherheitseinstellungen immer außer Kraft setzen.



Task-Leistensymbol





Wichtig

Diese Option steht nur zur Verfügung, wenn der Netzwerkadministrator sie über Richtlinieneinstellungen freigeschaltet hat.

Diese Option ist für Bitdefender Endpoint Security Tools for Windows Legacy nicht verfügbar.

Das Bitdefender Endpoint Security Tools-Symbol in der Task-Leiste weist Sie auf Probleme hin, die Ihren Computer beeinträchtigen, indem es sein Aussehen verändert:

-  Critical issues affect the security of the system.
-  Some issues affect the security of the system.




Beachten Sie

Der Netzwerkadministrator kann das Task-Leistensymbol ausblenden, wenn er möchte.

1.2. Das Hauptfenster

Im Hauptfenster von Accetta Bitdefender Endpoint Security Tools können Sie den Sicherheitsstatus überprüfen und Scan-Aufgaben ausführen. Und das alles mit nur wenigen Klicks. Die Konfiguration und Verwaltung der Sicherheit erfolgt per Fernzugriff durch Ihren Netzwerkadministrator.

Sie können die Benutzeroberfläche von Bitdefender Endpoint Security Tools über das Windows-Startmenü über den folgenden Pfad aufrufen: **Start** → **Alle Programme** → **Bitdefender Endpoint Security Tools** → **Sicherheitskonsole öffnen**. Noch schneller geht es mit einem Doppelklick auf Bitdefender Endpoint Security Tools  in der Task-Leiste.



Hauptfenster

Das Fenster ist in zwei Hauptbereiche aufgeteilt:

- [Statusbereich](#)
- [Ereignischronik](#)

1.2.1. Dem Statusbereich

Im **Statusbereich** finden Sie hilfreiche Informationen zur Sicherheit des Systems.



Statusbereich

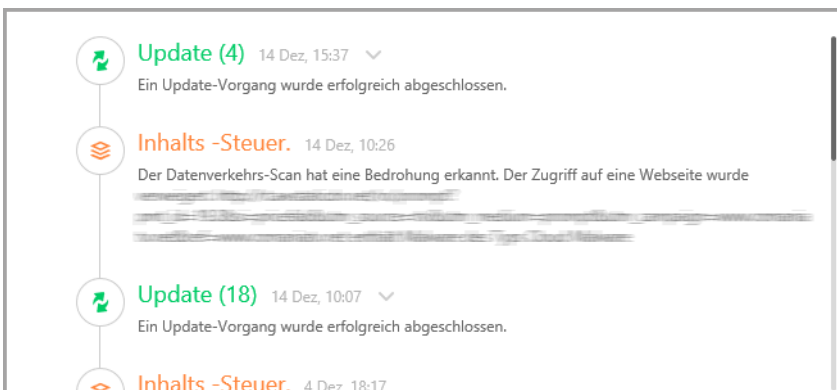
Sie können den aktuellen Sicherheitsstatus ganz leicht am Statussymbol links vom Statusbereich ablesen:

- **Grünes Häkchen.** Es liegen keine Probleme vor. Ihr Rechner und Ihre Daten sind geschützt.
- **Gelbes Ausrufezeichen.** Die Sicherheit Ihres Systems wird durch nicht-kritische Probleme beeinträchtigt.
- **Rotes X.** Die Sicherheit Ihres Systems wird durch kritische Probleme beeinträchtigt.

Zusätzlich zum Statussymbol wird ein Sicherheitsstatushinweis rechts vom Statusbereich angezeigt. Sie können die gefundenen Sicherheitsprobleme anzeigen, indem Sie auf den Statusbereich klicken. Bestehende Probleme werden von Ihrem Netzwerkadministrator behoben.

1.2.2. Ereignischronik


Bitdefender Endpoint Security Tools führt ein detailliertes Ereignisprotokoll über alle Aktivitäten der Software auf Ihrem Computer einschließlich der Aktivitäten, die von der Inhaltssteuerung überwacht werden.

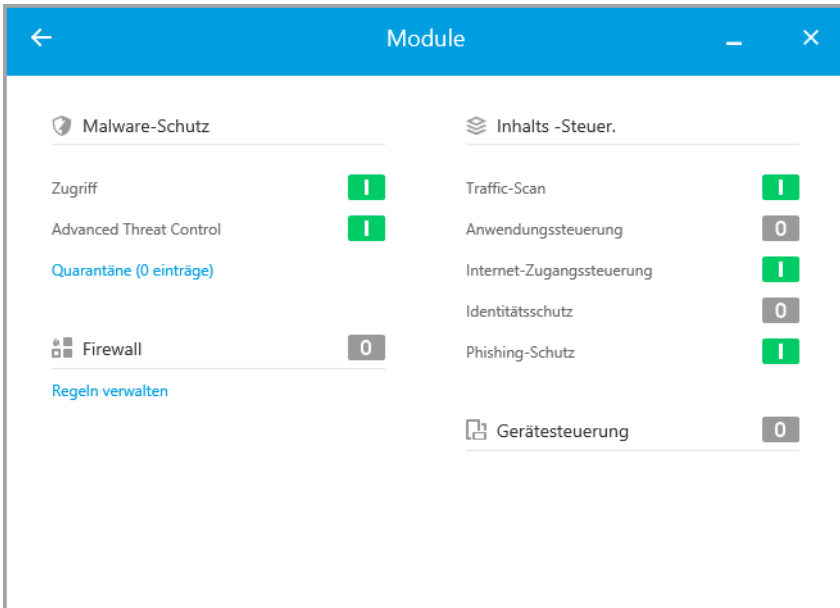


Ereignischronik

Die **Ereignis**-Zeitleiste ist ein wichtiges Hilfsmittel bei der Überwachung des Bitdefender-Schutzes. So können Sie beispielsweise einfach überprüfen ob ein Update erfolgreich durchgeführt wurde oder ob Malware auf Ihrem Computer entdeckt wurde.

1.3. Das Modulfenster

Das **Module**-Fenster zeigt nützliche Informationen über den Status und die Aktivität der installierten Sicherheitsmodule an. Klicken Sie zum Öffnen des **Module**-Fensters auf die **Module**-Schaltfläche  im Bitdefender Endpoint Security Tools-Hauptfenster.



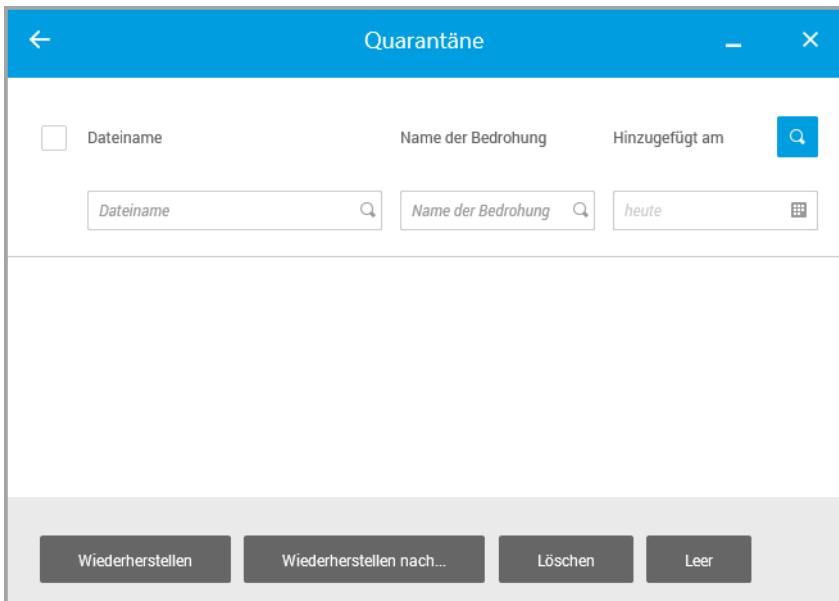
Module-Fenster

Malware-Schutz

Der Malware-Schutz bildet die Grundlage Ihrer Sicherheit. Bitdefender Endpoint Security Tools schützt Sie sowohl in Echtzeit als auch bei Bedarf vor allen Arten von Malware, so zum Beispiel vor Viren, Trojanern, Spyware, Adware usw.

- **Zugriff.** Zugriff-Scans verhindern, dass neue Malware auf das System gelangt, indem lokale und Netzwerk-Dateien gescannt werden, sobald auf sie zugegriffen wird (öffnen, verschieben, kopieren oder ausführen). Ferner werden Boot-Sektoren und potenziell unerwünschte Anwendungen (PUA) gescannt.

- **HyperDetect.** HyperDetect entdeckt komplexe Angriffe und verdächtige Aktivitäten schon vor der Ausführung. Diese Sicherheitsebene setzt auf maschinelle Lernmodelle und umfasst eine Technologie zur Erkennung von getarnten Angriffen.
- **Advanced Threat Control.** Es überwacht ständig alle Anwendungen, die auf dem Endpunkt laufen, auf Malware-artiges Verhalten. Advanced Threat Control wird automatisch versuchen, die gefundene Datei zu desinfizieren.
- **Quarantäne** zeigt eine Liste der Dateien in der Quarantäne einschließlich ihres ursprünglichen Speicherorts, des Datums und der Uhrzeit der Quarantäneaktion sowie des Sicherheitsstatus. Verwenden Sie die Schaltflächen unten, um die gewünschten Dateien zu löschen oder wiederherzustellen. Klicken Sie auf **Leeren**, um alle Dateien in Quarantäne zu löschen.



Quarantäne

Inhalts-Steuerung

Das Modul Inhaltssteuerung schützt Sie im Internet vor Phishing-Angriffen, Betrugsversuchen, Diebstahl vertraulicher Daten und nicht jugendfreien Inhalten.

Darüber hinaus enthält es umfangreiche Benutzersteuerungselemente, mit denen Netzwerkadministratoren die Einhaltung von Richtlinien zur Computer- und Internet-Nutzung sicherstellen können.

- **Datenverkehr-Scan.** Diese Komponente verhindert, dass Malware auf den Endpunkt heruntergeladen wird, indem eingehende E-Mails und der eingehende Internet-Datenverkehr in Echtzeit gescannt werden. Ausgehende E-Mails werden gescannt, um zu verhindern, dass Malware andere Endpunkte infiziert.
- **Anwendungs-Blacklist.** Diese Komponente verhindert, dass nicht zugelassene Anwendungen auf Ihr Unternehmensnetzwerk zugreifen. Es steht in der Verantwortung des Administrators, Regeln für die im Unternehmen zugelassenen Anwendungen aufzustellen.
- **Internet-Zugangssteuerung.** Diese Komponente nutzt vom Administrator festgelegte Regeln, um zu verhindern, dass gefährliche Websites aufgerufen werden.
- **Identitätsschutz.** Mit dieser Komponente kann der Administrator Regeln definieren, die eine unautorisierte Weitergabe von sensiblen Daten verhindern.
- **Phishing-Schutz.** Diese Komponente blockiert automatisch bekannte Phishing-Seiten, um zu verhindern, dass Benutzer unbeabsichtigt persönliche oder vertrauliche Informationen an Online-Betrüger weitergeben.
- **Network Attack Defense.** Network Attack Defense erkennt Verfahren für Angriffe auf das Netzwerk, die Angreifern Zugriff auf bestimmte Endpunkte verschaffen sollen, so zum Beispiel Brute-Force-Angriffe, Netzwerk-Exploits und Passwortdiebstahl.



Beachten Sie

Dieses Modul ist für Bitdefender Endpoint Security Tools for Windows Legacy nicht verfügbar.

Firewall

Die Firewall schützt Sie, wenn Sie mit Netzwerken und dem Internet verbunden sind, indem sie Verbindungsversuche filtert und verdächtige oder gefährliche Verbindungen blockiert.



Beachten Sie

Dieses Modul ist für Bitdefender Endpoint Security Tools for Windows Legacy nicht verfügbar.

Gerätesteuerung

Hiermit kann mithilfe von in Richtlinien festgelegten Blockier-Regeln und Ausschlüssen verhindert werden, dass sensible Daten unbefugt weitergegeben werden und Infektionen über externe Datenträger ins Netzwerk gelangen. Dies ist für eine große Bandbreite an Gerätearten möglich. Es steht in der Verantwortung des Administrators, die Berechtigungen für die folgenden Arten von Geräten zu verwalten:

- Bluetooth-Adapter
- CDROM-Geräte
- Diskettenlaufwerke
- IEEE 1284.4
- IEEE 1394
- Bildgebende Geräte
- Modems
- Bandlaufwerke
- Windows Mobile
- COM/LPT-Ports
- SCSI Raid
- Drucker
- Netzwerkadapter
- WLAN-Netzwerkkarten
- Interne und externe Speichermedien



Beachten Sie

Dieses Modul ist für Bitdefender Endpoint Security Tools for Windows Legacy nicht verfügbar.

Anwendungssteuerung

Das Anwendungssteuerungsmodul verhindert, dass nicht autorisierte Anwendungen und Prozesse auf dem Endpunkt ausgeführt werden. Die Anwendungssteuerung verringert die Häufigkeit und Schwere von Malware-Vorfällen. Es verkleinert die Angriffsfläche und schließt Sicherheitslücken, indem es nicht erwünschte Anwendungen aus Ihrem Netzwerk fernhält.



Beachten Sie

Dieses Modul ist für Bitdefender Endpoint Security Tools for Windows Legacy nicht verfügbar.

Sandbox Analyzer

Das Sandbox Analyzer-Modul bietet hohe Sicherheit vor komplexen Bedrohungen, indem automatische, detaillierte Analysen verdächtiger Dateien durchgeführt werden; selbst solcher Dateien, die noch keine Signatur von den Bitdefender-Malware-Schutz-Engines erhalten haben. In der Sandbox Analyzer kommen verschiedene eigenentwickelte Technologien zum Einsatz, mithilfe derer Schad-Code in einer abgeschlossenen von Bitdefender gehosteten virtuellen Umgebung ausgeführt, anschließend das Verhalten analysiert und jede noch so kleine Veränderung am System, die auf schädliche Aktivitäten hindeuten könnten, gemeldet wird.



Beachten Sie

Dieses Modul ist für Bitdefender Endpoint Security Tools for Windows Legacy nicht verfügbar.

Laufwerksverschlüsselung

Mit dem Laufwerksverschlüsselungsmodul können Sie auf Windows-Maschinen BitLocker verwalten und so Laufwerke vollständig verschlüsseln. Sie können Laufwerke (ob boot-fähig oder nicht) mit nur einem Klick verschlüsseln und entschlüsseln. Dabei übernimmt GravityZone die meiste Arbeit. Sie selbst müssen kaum etwas tun. Außerdem werden in GravityZone die Wiederherstellungsschlüssel gespeichert, die zur Entschlüsselung der Laufwerke benötigt werden, falls der Benutzer mal das Passwort vergessen sollte.



Beachten Sie

Dieses Modul ist für Bitdefender Endpoint Security Tools for Windows Legacy nicht verfügbar.

EDR-Sensor

Der EDR-Sensor (Endpoint Detection and Response) erfasst, verarbeitet und berichtet über Daten zum Verhalten von Endpunkten und Anwendungen. Manche Informationen werden lokal verarbeitet, während komplexere Datensätze an eine Backend-Komponente von GravityZone weitergeleitet werden.

Das Modul benötigt nur wenig Netzwerkbandbreite und schont die Hardwareressourcen.

**Beachten Sie**

Dieses Modul ist für Bitdefender Endpoint Security Tools for Windows Legacy nicht verfügbar.


Patch-Management

Das Patch Management sorgt dafür, das Betriebssystem und andere Anwendungen immer auf dem neuesten Stand sind. Dieses Modul beinhaltet verschiedene Funktionen, darunter Patch-Scans auf Knopfdruck oder nach Plan, automatisches/manuelles Einspielen von Patches und Berichte zu fehlenden Patches.

**Beachten Sie**

Dieses Modul ist für Bitdefender Endpoint Security Tools for Windows Legacy nicht verfügbar.

1.4. Aktionsmenü

Wenn Sie eine Scan-Aufgabe definieren oder ausführen möchten, klicken Sie auf die Schaltfläche **Aktionen** ; dadurch öffnet sich das Menü **Aktionen**. Hier können Sie auch nach Updates suchen.



Aktionsmenü

Quick-Scan

Verwendet Cloud-Scans, um im System verborgene Malware zu finden. Die Ausführung eines Quick Scans dauert im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virenskan in Anspruch nehmen würde.

System-Scan

Durchsucht den gesamten Computer nach allen Typen von Malware, die ein Sicherheitsrisiko darstellen, so z. B. Viren, Spyware, Adware, Rootkits usw.

Benutzerdefinierter Scan

Sie können wählen, welche Speicherorte Sie scannen möchten und Scan-Optionen konfigurieren.

Auf Updates prüfen

Wenn ein Update gefunden wird, werden Sie abhängig von den von Ihrem Netzwerkadministrator konfigurierten Update-Einstellungen entweder aufgefordert, dies zu bestätigen, oder das Update wird automatisch durchgeführt.

2. SCANNEN AUF MALWARE

Die Hauptaufgabe von Bitdefender Endpoint Security Tools ist es, Ihren Computer frei von Malware zu halten. Dies geschieht vornehmlich durch Echtzeit-Scans aller aufgerufenen Dateien, E-Mail-Nachrichten und aller neuen Dateien, die auf Ihren Computer heruntergeladen oder kopiert werden. Neben dem Echtzeitschutz können auch Scans durchgeführt werden, die etwaige Malware auf Ihrem Computer erkennen und entfernen.

Sie können den Computer jederzeit scannen, indem Sie die Standard-Aufgaben oder Ihre eigenen Scan-Aufgaben (benutzerdefinierte Aufgaben) ausführen. Die Scan-Aufgaben beinhalten die Scan-Optionen und die Objekte, die gescannt werden sollen. Wenn Sie bestimmte Bereiche Ihres Computers scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierten Scan konfigurieren und ausführen.

Während der Scan ausgeführt wird, können Sie den Fortschritt in der **Ereignisse**-Zeitleiste verfolgen.

2.1. Scannen von Dateien und Ordnern

Wenn Sie den Verdacht hegen, dass Dateien und Verzeichnisse infiziert sein könnten, sollten Sie einen Scan durchführen. Rechtsklicken Sie auf die zu scannende Datei oder Verzeichnis und wählen Sie **Mit Bitdefender Endpoint Security Tools scannen**. Der Scan wird gestartet, und Sie können den Fortschritt in der **Ereignisse**-Zeitleiste verfolgen.

Am Ende des Scans wird das Ergebnis angezeigt. Detailliertere Informationen erhalten Sie, wenn Sie auf **Protokoll anzeigen** klicken.

2.2. Durchführen von Quick Scans

Beim **Quick Scan** wird das sog In-the-Cloud-Verfahren angewandt, um auf Ihrem System laufende Malware aufzuspüren. Die Ausführung eines Quick Scans dauert im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virenskan in Anspruch nehmen würde.

Quick Scan ist so vorkonfiguriert, dass folgende Scans möglich sind:

- Laufende Prozesse, **Startsektor** und Registry.
- Kritische Speicherbereiche

- Nur neue und geänderte Dateien
- Für **Rootkits**, **Adware**, **Spyware** und Dialer-Programme in kritischen Betriebssystembereichen wie: %windir%\system32\, %temp%, /etc, /lib.
- Für potenziell unerwünschte Anwendungen (PUA).

Um einen Quick Scan auszuführen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender Endpoint Security Tools-Fenster.
2. Klicken Sie oben rechts auf die Schaltfläche **Aktionen**.
3. Klicken Sie auf **Quick Scan**.
4. Warten Sie, bis der Scan abgeschlossen ist. In der Zeitleiste wird der Fortschritt des Scans angezeigt. Nach Abschluss des Scans können Sie auf **Protokoll anzeigen** klicken, um detailliertere Ergebnisse zu sehen.

2.3. Einen Vollständigen Scan ausführen

Der **vollständige Scan** scannt den gesamten Computer nach allen Malware-Typen, die ein Sicherheitsrisiko darstellen, so zum Beispiel Viren, Spyware, Adware, Rootkits usw.



Beachten Sie

Da ein **vollständiger Scan** das gesamte System scannt, kann er eine Weile dauern. Es empfiehlt sich daher, diese Aufgabe durchzuführen, wenn Sie den Computer nicht benötigen.

Wenn Sie bestimmte Bereiche Ihres Computers scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierten Scan konfigurieren und ausführen. Für weitere Informationen lesen Sie bitte [„Konfigurieren und Ausführen eines benutzerdefinierten Scans“](#) (S. 15).

Stellen Sie vor der Durchführung eines vollständigen Scans sicher, dass Bitdefender Endpoint Security Tools über die aktuellsten Malware-Signaturen verfügt. Ihren Computer unter Verwendung einer veralteten Signaturrendatenbank zu prüfen, kann Bitdefender Endpoint Security Tools daran hindern neue Maleware, welche seit dem letzten Update gefunden wurde, zu erkennen. Für weitere Informationen lesen Sie bitte [„Aktualisierung“](#) (S. 25).

Der **Vollständige Scan** ist so konfiguriert, dass folgende Scans möglich sind:

- Laufende Prozesse, **Startsektor** und Registry.

- E-Mail-Archive und Netzwerkdateien auf allen Laufwerken und Wechsellaufwerken.
- Für **Rootkits**, **Adware**, **Spyware**, Keylogger und Dialer-Anwendungen auf allen Laufwerken und Wechsellaufwerken.
- Für potenziell unerwünschte Anwendungen (PUA)
- Browser-Cookies

Um einen Vollständiger Scan auszuführen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender Endpoint Security Tools-Fenster.
2. Klicken Sie oben rechts auf die Schaltfläche **Aktionen** .
3. Klicken Sie auf **Vollständiger Scan**.
4. Warten Sie, bis der Scan abgeschlossen ist. In der Zeitleiste wird der Fortschritt des Scans angezeigt. Wenn Sie auf **Details anzeigen** klicken, werden während des Scans Details dazu angezeigt. Sie können den Scan auch unterbrechen, verschieben oder anhalten.
5. Bitdefender Endpoint Security Tools wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen. Nach Abschluss des Scans können Sie auf **Protokoll anzeigen** klicken, um detailliertere Ergebnisse zu sehen.

2.4. Konfigurieren und Ausführen eines benutzerdefinierten Scans

Um einen Malware-Scan im Detail zu konfigurieren und dann auszuführen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Hauptfenster von Bitdefender Endpoint Security Tools.
2. Klicken Sie oben rechts auf die Schaltfläche **Aktionen** .
3. Klicken Sie auf **Neuer benutzerdefinierter Scan**. Das Fenster **Benutzerdefinierter Scan** wird geöffnet.
4. Konfigurieren Sie die Scan-Optionen: **Aggressiv**, **Normal**, **Tolerant**, **Benutzerdefiniert**. Die Beschreibung unter der jeweiligen Option hilft Ihnen, die Scan-Option zu wählen, die für Ihre Bedürfnisse am besten geeignet ist.
5. Wählen Sie im linken Fenster das Ziel des Scans.

6. Wenn Sie das ansprechende Kästchen markieren, können Sie den Scan auch mit niedriger Priorität ausführen lassen. Das verringert die Priorität des Scan-Prozesses. Dadurch können andere Programme schneller laufen, der Scan dauert aber länger.

Nachdem sie den benutzerdefinierten Scan konfiguriert haben, können Sie ihn als Favoriten speichern. Geben Sie dazu einen Namen ein und klicken Sie auf die Schaltfläche **Favorit**.

Erfahrene Benutzer können die Scan-Einstellungen von Bitdefender Endpoint Security Tools nutzen. Um die Scan-Optionen im Detail zu konfigurieren, klicken Sie auf **Benutzerdefiniert** und dann auf **Einstellungen**.

Alternativ können Sie über das Befehlszeilentool des Produkts einen benutzerdefinierten Scan konfigurieren und ausführen. Weitere Einzelheiten finden Sie im Kapitel „[Verwenden der Befehlszeilenoberfläche](#)“ (S. 29).

2.4.1. Dateitypen

Im Reiter **Dateitypen** können Sie festlegen, welche Dateien gescannt werden sollen. Sie können den Sicherheitsagenten so einrichten, dass Scans entweder für alle Dateien (unabhängig von der Dateierweiterung), oder nur für Anwendungsdateien oder nur für bestimmte Dateierweiterungen, die Sie für gefährlich erachten, durchgeführt werden.

Das Scannen aller Dateien bietet den besten Schutz, während das Scannen nur von Anwendungen verwendet wird, um einen schnelleren Scan durchzuführen. Anwendungen (oder Programmdateien) sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen. Diese Kategorie beinhaltet die folgenden Dateierweiterungen:

```
386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt;
accdu; acl; acr; action; ade; adp; air; app; as; asd; asp;
awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl;
csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm;
dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv;
hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar;
js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr;
mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg;
msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg;
ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx;
ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg;
```

pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox;
rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm;
snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe;
vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf;
xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsx;
xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

Scan-Optionen für Archive

Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für Ihre Systemsicherheit. Die Malware kann Ihr System nur beeinflussen, wenn die infizierte 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.

E-Mail-Archive scannen

Wählen Sie diese Option, wenn Sie möchten, dass E-Mail-Dateien und E-Mail-Datenbanken (Dateiformate wie EML, MSG, PST, DBX, MBX, TBB usw.) gescannt werden.

2.4.2. Was soll gescannt werden?

Markieren Sie im Reiter **Scan** die entsprechenden Kästchen, um die gewünschten Scan-Optionen zu aktivieren.

Boot-Sektoren scannen

Sie können Bitdefender Endpoint Security Tools einstellen, damit die Boot-Sektoren gescannt werden. Dieser Sektor der Festplatte beinhaltet den notwendigen Computercode um den Boot-Prozess zu starten. Wenn ein Virus den Boot-Sektor infiziert, könnte das Laufwerk unzugänglich werden und es könnte Ihnen nicht mehr möglich sein, Ihr System zu starten und auf Ihre Daten zuzugreifen.

Nach Rootkits suchen

Wählen Sie diese Option, um nach **Rootkits** und Objekten zu suchen, die mit dieser Art von Software versteckt werden.

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.

Nach Keyloggern suchen

Wählen Sie diese Option, um nach [Keylogger](#)-Software zu suchen.

Auf potenziell unerwünschten Anwendungen (PUA) scannen

Eine potenziell unerwünschte Anwendung (PUA) ist ein Programm, das auf dem PC vermutlich nicht erwünscht ist und häufig in Verbindung mit Freeware installiert wurde. Diese Art von Programmen kann ohne Zustimmung des Benutzers installiert werden (wird auch als Adware bezeichnet) oder wird standardmäßig bei der Express-Installation mitinstalliert (werbeunterstützt). Diese Programme können Pop-up-Werbung anzeigen, unerwünschte Symbolleisten im Standard-Browser installieren oder Hintergrundprozesse ausführen und so den PC verlangsamen.

Nur neue und geänderte Dateien

Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.

Cookies scannen

Wählen Sie diese Option, um die Cookies zu scannen, die von Ihrem Browser auf Ihrem Computer gespeichert werden.

2.4.3. Aktionen bei Fund

Stellen Sie im Reiter **Aktionen** die Aktion ein, die auf gefundene Dateien angewendet werden soll (falls eine angewendet werden soll).

Infizierte Dateien

Als infiziert eingestufte Dateien stimmen mit einer Malware-Signatur der Bitdefender Malware-Signaturen-Datenbank überein.

Verdächtige Dateien

Dateien werden von der heuristischen Analyse als verdächtig klassifiziert. Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist.

Rootkits

Rootkits sind spezielle Software-Werkzeuge, die verwendet werden, um Dateien vor dem Betriebssystem zu verbergen. Obwohl sie nicht zwangsläufig als schädlich anzusehen sind, werden Rootkits häufig genutzt, um Malware zu verbergen oder Eindringlinge im System zu tarnen.

Aktionen ausführen

Je nach Art der gefundenen Dateien stehen eine oder mehrere der folgenden Optionen zur Verfügung:

Löschen

Infizierte Dateien werden von der Festplatte entfernt.

Falls infizierte Dateien zusammen mit nicht infizierten Dateien in einem Archiv gespeichert sind, wird Bitdefender Endpoint Security Tools 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.

Ignorieren

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.

Dateien in Quarantäne verschieben

Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko.

Desinfizieren

Entfernt den Malware-Code aus der infizierten Datei und rekonstruiert die ursprüngliche Datei.

2.5. Prüfen der Scan-Protokolle

Für jeden Scan wird ein Protokoll erstellt. 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 Hauptfenster heraus öffnen, indem Sie auf **Protokoll anzeigen** klicken.

Um die Scan-Protokolle zu einem späteren Zeitpunkt zu überprüfen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Hauptfenster von Bitdefender Endpoint Security Tools.
2. Klicken Sie auf die Schaltfläche **Filter**, um das **Filter**-Menü zu öffnen.
3. Klicken Sie auf die Schaltfläche **Malware-Schutz**. Hier können Sie alle Malware-Scan-Ereignisse finden, einschließlich der Bedrohungen, die während Zugriff-Scans, kürzlichen Scans und vom Benutzer gestarteten Scans gefunden wurden. Dazu kommen Statusänderungen für automatische Scans.
4. Klicken Sie auf ein Ereignis, um mehr darüber zu erfahren.
5. Um das Scan-Protokoll zu öffnen, klicken Sie auf **Protokoll anzeigen**. Das Scan-Protokoll wird angezeigt.

3. VERWENDUNG DER LAUFWERKSVERSCHLÜSSELUNG

Das Modul für die Laufwerksverschlüsselung ermöglicht durch vom Sicherheitsadministrator festgelegte Richtlinien eine vollständige Verschlüsselung von Laufwerken in Ihrem Windows-System.

3.1. Wie Sie Ihr System verschlüsseln

Wenn Ihrem Windows-System eine Verschlüsselungsrichtlinie zugewiesen ist:

1. Ein Konfigurationsfenster wird angezeigt, indem Sie aufgefordert werden, eines der Folgenden einzugeben:
 - Eine Persönliche Identifikationsnummer (PIN) im Fall, dass das System einen Trusted-Platform-Modul-Chip (TPM-Chip) hat (das ist bei neueren Laptops oft der Fall).



Beachten Sie

Wenn Ihr System ein funktionierendes TPM hat, kann Ihr Sicherheitsadministrator eine Richtlinie zur automatischen Verschlüsselung der Laufwerke konfigurieren, ohne dass Sie eine PIN eingeben müssen.

- Ein Passwort im Fall, dass das System keinen TPM-Chip hat. Das Passwort ist auch nötig, wenn das TPM nicht funktioniert oder nicht von Bitdefender Endpoint Security Tools erkannt wird.

Laufwerksverschlüsselung

Verschlüsselungspasswort festlegen

Legen Sie unter Verwendung des US-amerikanischen Tastaturlayouts (EN-US) ein Passwort fest. Dieses wird zum Starten des Betriebssystems oder zum Entsperren der Volume benötigt.

Die Verschlüsselung ist ein einmaliger Vorgang und Sie können währenddessen wie gewohnt weiterarbeiten.

Geben Sie das Verschlüsselungspasswort für das Laufwerk C: ein. Das Passwort werden Sie zur Entsperrung des Laufwerks wieder brauchen.

Passwort auswählen:

Passwort wiederholen:

Passwortanforderungen:

- Mindestens 8 Zeichen
- Sollte Groß- und Kleinbuchstaben enthalten
- Sollte eine Zahl enthalten

[Ablehnen](#)

2. Klicken Sie auf den Button **Speichern**. Der Verschlüsselungsvorgang startet automatisch, zuerst auf dem Boot-Laufwerk.

Sie können die Verschlüsselung auf später verschieben, indem Sie auf **Verwerfen** klicken. Das Fenster wird dann nach einer gewissen Zeit wieder angezeigt, und Sie werden dann aufgefordert, eine PIN bzw. ein Passwort für die Verschlüsselung zu konfigurieren.

Ein(e) einzige(s) PIN/Passwort genügt, um alle Laufwerke (bootfähig oder nicht) auf Desktops oder Laptops zu verschlüsseln. Wechseldatenträger werden nicht verschlüsselt. Weitere Informationen zur Konfiguration von Verschlüsselungs-PIN/Passwörtern finden Sie in [diesem Artikel](#).

Nach der Verschlüsselung müssen Sie je nach der Sicherheitsrichtlinie, die Ihrem System zugewiesen ist, ggf. bei jedem Systemstart das Passwort bzw. die PIN eingeben.



Falls Sie die PIN bzw. das Passwort vergessen, wenden Sie sich an Ihren Sicherheitsadministrator.

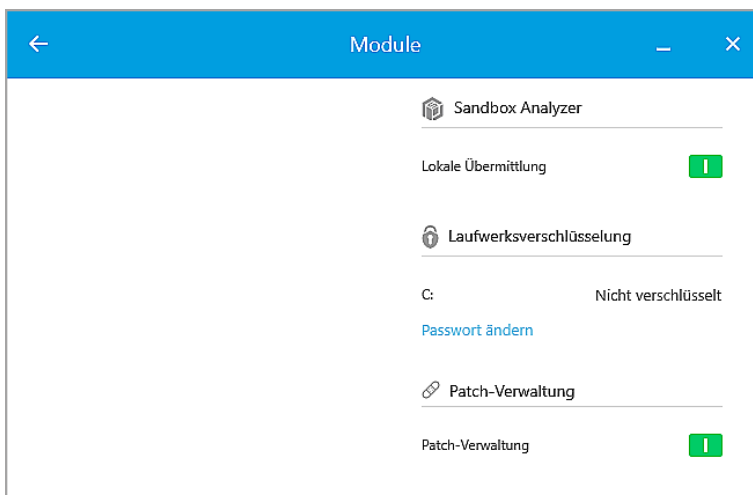
3.2. Entschlüsselung Ihres Systems

Wenn eine Entschlüsselungsrichtlinie angewendet wird, werden die verschlüsselten Laufwerke automatisch entschlüsselt. Sie brauchen dafür nichts zu tun. Solange eine Verschlüsselungsrichtlinie jedoch aktiv ist, können Sie Ihr System nicht selbst entschlüsseln.

3.3. Überprüfung des Verschlüsselungsstatus

So überprüfen Sie den Verschlüsselungsstatus Ihres Systems:

1. Doppelklicken Sie in der Taskleiste auf das Symbol  um die Benutzeroberfläche von Bitdefender Endpoint Security Tools aufzurufen.
2. Klicken Sie rechts oben auf , um das Fenster **Module** zu öffnen.
3. Im Bereich **Laufwerkverschlüsselung** wird angezeigt, welche Laufwerke verschlüsselt sind und welche nicht.



3.4. Ändern der/des Verschlüsselungs-PIN/Passworts

So ändern Sie die/das Verschlüsselungs-PIN/Passwort:

1. Klicken Sie im Hauptfenster von Bitdefender Endpoint Security Tools auf den Namen des verschlüsselten Laufwerks.
2. Klicken Sie auf **Passwort ändern**.
3. Geben Sie im Konfigurationsfenster die neue PIN bzw. das neue Passwort ein.
4. Klicken Sie auf den Button **Speichern**.

4. AKTUALISIERUNG

In einer Welt, in der Internet-Kriminelle immer neue Wege finden, um Ihnen zu schaden, ist es von größter Wichtigkeit, dass Sie Ihre Sicherheitslösung zu jeder Zeit auf dem neuesten Stand halten, um stets einen Schritt voraus zu sein.

Falls Sie über eine Breitbandverbindung oder eine DSL-Verbindung verfügen, arbeitet Bitdefender Endpoint Security Tools eigenständig. Standardmäßig sucht die Software nach Updates, wenn Sie Ihren Computer einschalten und danach einmal pro **Stunde**.



Beachten Sie

Die standardmäßige Frequenz für automatische Updates kann von Ihrem Netzwerkadministrator angepasst werden.

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

Falls Sie sich per Einwahl mit dem Internet verbinden, ist es sinnvoll, regelmäßig ein manuelles Bitdefender-Update durchzuführen. Für weitere Informationen lesen Sie bitte „[Durchführung eines Updates](#)“ (S. 26).

4.1. Arten von Updates

Folgende Update-Arten gibt es:

- **Updates der Malware-Signaturen** - Immer wenn neue Bedrohungen auftreten, müssen die Dateien mit den Malware-Signaturen aktualisiert werden, um einen durchgängigen und aktuellen Schutz zu gewährleisten.
- **Produkt-Updates** - wenn eine neue Version auf dem Markt erscheint, enthält diese zur Leistungssteigerung des Produkts neue Funktionen und Scantechniken.

Bei einem Produkt-Upgrade handelt es sich um eine neue Hauptversion der Software.

4.2. Überprüft, ob Ihr Schutz auf dem neuesten Stand ist

Um zu überprüfen, ob Ihr Schutz auf dem neuesten Stand ist, gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf das Bitdefender Endpoint Security Tools-Symbol in der Task-Leiste und wählen Sie **Über**.
2. Der Update-Status und der Zeitpunkt der letzten Update-Überprüfung und Update-Installation werden angezeigt.

Um ausführliche Informationen zu Ihren letzten Updates zu erhalten, rufen Sie die Update-Ereignisse auf:

1. Klicken Sie im Hauptfenster auf die Schaltfläche **Filter**, um das **Filters**-Menü aufzurufen.
2. Klicken Sie auf die Schaltfläche **Update**. In der **Ereignisse**-Zeitleiste werden die neuesten Updates angezeigt.

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.

4.3. Durchführung eines Updates

Sie benötigen eine Internet-Verbindung, um Updates durchzuführen.

So starten Sie ein Update:

- Klicken Sie doppelt auf das Bitdefender Endpoint Security Tools-Symbol in der **Task-Leiste**.
- Klicken Sie auf die Schaltfläche **Aktionen**, um das Menü **Aktionen** zu öffnen.
- Klicken Sie auf **Auf Updates überprüfen**. Das Update-Modul verbindet sich mit dem Bitdefender-Update-Server und sucht nach verfügbaren Updates.
- Wenn ein Update gefunden wird, werden Sie abhängig von den von Ihrem Netzwerkadministrator konfigurierten Update-Einstellungen entweder aufgefordert, dies zu bestätigen, oder das Update wird automatisch durchgeführt.



Wichtig

Falls nötig starten Sie das System sobald es Ihnen möglich ist neu. Wir empfehlen, das so bald wie möglich zu tun.

5. EREIGNISANZEIGE

Bitdefender Endpoint Security Tools zeigt ein detailliertes Ereignisprotokoll aller Aktivitäten der Software auf Ihrem Computer einschließlich der Computer-Aktivitäten, die von der Inhaltssteuerung aufgezeichnet wurden, und der Anwendungen, die von der Anwendungssteuerung blockiert wurden. Die **Ereignisse**-Zeitleiste ist ein wichtiges Hilfsmittel bei der Überwachung des Bitdefender-Schutzes. So können Sie beispielsweise einfach überprüfen ob ein Update erfolgreich durchgeführt wurde, ob Malware auf Ihrem Computer entdeckt wurde usw. Um das Ereignisprotokoll aufzurufen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Hauptfenster von Bitdefender Endpoint Security Tools.
2. Alle Ereignisse werden in der **Ereignisse**-Zeitleiste aufgeführt.
3. Klicken Sie auf die Schaltfläche **Filter**, um das **Filter**-Menü zu öffnen.
4. Wählen Sie die Ereigniskategorie aus dem Menü. Ereignisse sind in die folgenden Kategorien unterteilt:
 - **Allgemeine Einstellungen**
 - **Malware-Schutz**
 - **Firewall**
 - **Update (Aktualisierung)**
 - **Inhalts-Steuerung**
 - **Gerätesteuerung**
 - **Anwendungssteuerung**
 - **Sandbox Analyzer**
 - **Laufwerksverschlüsselung**

Sie erhalten die folgenden Informationen zu jedem Ereignis: eine Kurzbeschreibung; die Aktion, die Bitdefender beim Auftreten des Ereignisses durchgeführt hat; der Zeitpunkt des Ereignisses. Weitere Informationen zu einem bestimmten Ereignis in der Liste erhalten sie, indem Sie auf **Protokoll anzeigen** klicken.

Sie können Ereignisse auch nach der Wichtigkeit für die Sicherheitsstufe filtern. Es gibt drei Ereignistypen:



zeigt erfolgreiche Vorgänge an.



zeigt nicht-kritische Probleme an.



zeigt kritische Probleme an.



Einige der kritischen und nicht kritischen Probleme in der **Ereignis**-Zeitleiste werden zur Problembeseitigung den empfohlenen Aktionen zugeordnet.

6. VERWENDEN DER BEFEHLSZEILENOBERFLÄCHE

Mit Bitdefender Endpoint Security Tools können Sie automatisch lokale Bedarf-Scan-Aufgaben und Updates über die Produktkonsole ausführen. Dabei handelt es sich um eine Befehlszeilenoberfläche, die Sie im Produktinstallationsordner auf Ihren Windows-Computern finden können.

Die BEST-Befehlszeilenoberfläche verfügt über zwei Funktionsmodi:

- **Ausführung mehrerer Befehle gleichzeitig.** Die Modus verwendet eine eigene Befehlszeilenoberfläche und erlaubt Ihnen die Eingabe von Befehlen und den Erhalt von Ergebnissen bis Sie die Oberfläche wieder verlassen.

Gehen Sie folgendermaßen vor, um auf diesem Modus zuzugreifen:

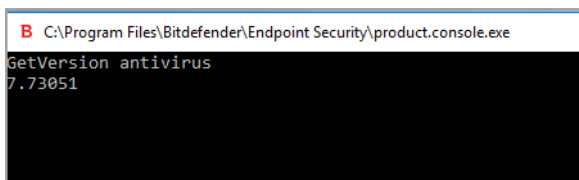
1. Öffnen Sie `c:\Programme\Bitdefender\Endpoint Security` bzw. den Ordner, in dem BEST installiert wurde.
2. Suchen Sie die ausführbare Datei **product.console** und führen Sie sie mit einem Doppelklick aus. Die Befehlszeilenoberfläche wird geöffnet.
3. Führen Sie den gewünschten Befehl aus.

Beispiel:

```
GetVersion antivirus
```

Das zurückgegebene Ergebnis ist die Versionsnummer der Malware-Schutz-Signaturen.

4. Führen Sie den Befehl `exit` aus, um die Befehlszeilenoberfläche zu schließen.



```
C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
GetVersion antivirus
7.73051
```

- **Ausführung einzelner Befehle.** Dieser Modus nutzt eine Befehlseingabeaufforderung und kehrt nach Ausführung des Befehls zur Systemeingabeaufforderung zurück.

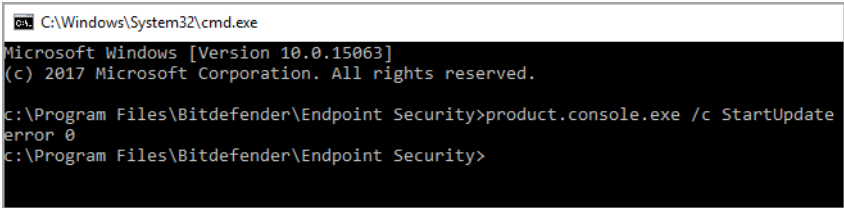
Gehen Sie folgendermaßen vor, um auf diesem Modus zuzugreifen:

1. Öffnen Sie die Befehlseingabeaufforderung (`cmd.exe`).
2. Navigieren Sie mit dem `cd`-Befehl zum Bitdefender Endpoint Security Tools-Installationsordner.
3. Führen Sie den gewünschten Befehl aus.

Beispiel:

```
C:\Program Files\Bitdefender\Endpoint Security>
product.console.exe /c StartUpdate
```

4. Bei erfolgreicher Ausführung des Befehls lautet das zurückgegebene Ergebnis `error 0`.



```
cmd C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

c:\Program Files\Bitdefender\Endpoint Security>product.console.exe /c StartUpdate
error 0
c:\Program Files\Bitdefender\Endpoint Security>
```

6.1. Unterstützte Befehle

Die Befehlszeilenoberfläche unterstützt eine Reihe von Befehlen. Einige dieser Befehle erfordern zur Rückgabe von gültigen Ergebnissen Parameter.

Für alle Beispiele in diesem Bereich wird die Produktkonsole aus dem BEST-Installationsordner verwendet.

GetUpdateStatus `product|antivirus`

Abfragen von Informationen zu dem/den letzten Update(s).

Dieser Befehl erfordert einen dieser Parameter:

- `product` – bezieht sich auf die BEST-Version.

- `antivirus` – bezieht sich auf die Version der Malware-Schutz-Signaturen.

Beispiel:

```

B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
GetUpdateStatus product
lastSucceededTime: 1504513705
lastAttemptedTime: 1504513705
lastError: 0
GetUpdateStatus antivirus
lastSucceededTime: 1505739144
lastAttemptedTime: 1505739144
lastError: 0
    
```

GetVersion `product|antivirus`

Abrufen von Informationen zur aktuellen Produktversion.

Dieser Befehl erfordert einen dieser Parameter:

- `product` – bezieht sich auf die BEST-Version.
- `antivirus` – bezieht sich auf die Version der Malware-Schutz-Signaturen.

Beispiel:

```

B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
GetVersion product
6.2.24.938
GetVersion antivirus
7.73205
    
```

IsUpdateInProgress

Überprüfen, ob gerade ein Produktupdate durchgeführt wird.

Ausgabewert:

- `true` - es wird gerade ein Produktupdate durchgeführt.
- `false` - es wird gerade kein Produktupdate durchgeführt.

Beispiel:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
IsUpdateInProgress
false
```

IsUpdateRestartNeeded

Überprüfen Sie, ob für einen Computer nach dem Update ein Systemneustart erforderlich ist.

Ausgabewert:

- true - für den Computer ist nach dem Update ein Systemneustart erforderlich.
- false - für den Computer ist nach dem Update kein Systemneustart erforderlich.

Beispiel:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
IsUpdateRestartNeeded
false
```

StartUpdate

Starten Sie ein Update und erhalten Sie das Ergebnis, ohne auf den Abschluss der Aufgabe warten zu müssen.

Beispiel:

```
StartUpdate
```

Ausgabeformat: error 0 (erfolgreiche Ausführung des Befehls)

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
StartUpdate
error 0
```

FileScan.OnDemand.RunScanTask custom [option]

Startet einen Bedarf-Scan und zeigt den Pfad zum Scan-Protokoll und eine Zusammenfassung des Scans an.

Dieser Befehl erfordert den Parameter `custom`, bei Bedarf gefolgt von einer oder mehreren Optionen. Zum Beispiel:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0-0-0\1505742554_1_01.xml
Scanned items: 990886
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

Mit den Optionen können Sie eine benutzerdefinierte Scan-Aufgabe anlegen. Diese Optionen sind nicht zwingend erforderlich.

Jede Option hat zwei oder mehr verfügbare Werte, Sie können jedoch nur einen Wert verwenden.

Wird für den Befehl `FileScan.OnDemand.RunScanTask` keine Option festgelegt, wird für den benutzerdefinierten Scan der Standardwert für diese Option verwendet. Wenn Sie zum Beispiel diesen Befehl ohne Erwähnung der Option `scanKeyloggers` ausführen, wird Bitdefender Endpoint Security Tools dennoch nach Keyloggern scannen, wie im Standardwert (`true`) für `scanKeyloggers` festgelegt.



Beachten Sie

Es gibt keine spezifischen Befehle für **Quick Scan** oder **Vollständiger Scan**. Sie können jedoch `FileScan.OnDemand.RunScanTask` konfigurieren, um

entweder nur die Betriebssystemsbereiche oder das gesamte System mit allen Optionen aktiviert zu scannen.

Optionen

path="<path>"

Geben Sie den Pfad für das Scan-Ziel ein. Verwenden Sie path="<path1>" path="<path2>", um mehrere Pfade anzugeben.

Beispiel:

```
FileScan.OnDemand.RunScanTask custom path="C:\Program Files"
```

```
FileScan.OnDemand.RunScanTask custom path="C:\Program Files"
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0-0\1505746495_1_01.xml
Scanned items: 74074
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

infectedAction1=ignore|disinfect|disinfectOnly|delete|quarantine

Legen Sie die erste Aktion fest, die beim Fund einer infizierten Datei ausgeführt werden soll: ignorieren, desinfizieren, löschen oder in die Quarantäne verschieben. Sie können diese Aktion in Kombination mit infectedAction2 verwenden.

Standardwert: disinfect

Beispiel:

```
FileScan.OnDemand.RunScanTask custom path="C:\Program Files\Common Files" infectedAction1=ignore
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0-0\1505813252_1_01.xml
Scanned items: 5542
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

infectedAction2=ignore|disinfect|disinfectOnly|delete|quarantine

Legen Sie die zweite Aktion fest, die beim Fund einer infizierten Datei ausgeführt werden soll, falls die erste Aktion fehlschlägt.

Standardwert: quarantine

Beispiel:

```
FileScan.OnDemand.RunScanTask custom infectedAction1=disinfect infectedAction2=quarantine
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1505824102_1_01.xml
Scanned items: 500139
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

suspiciousAction1=ignore|delete|quarantine

Legen Sie die erste Aktion fest, die beim Fund einer verdächtigen Datei ausgeführt werden soll. Sie können diese Aktion in Kombination mit `suspiciousAction2` verwenden.

Standardwert: ignore

Beispiel:

```
FileScan.OnDemand.RunScanTask custom path="C:\Program Files\Common Files" suspiciousAction1=quarantine
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1505824920_1_01.xml
Scanned items: 5542
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

suspiciousAction2=ignore|delete|quarantine

Legen Sie die zweite Aktion fest, die beim Fund einer verdächtigen Datei ausgeführt werden soll, falls die erste Aktion fehlschlägt.

Standardwert: ignore

Beispiel:

```
FileScan.OnDemand.RunScanTask custom path="C:\Users" suspiciousAction1=delete suspiciousAction2=quarantine
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1505825170_1_01.xml
Scanned items: 54455
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanBootSectors=true|false

Die Bootsektoren auf Ihrer Festplatte scannen.

Standardwert: false

Beispiel:


```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom scanBootSectors=true
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506073447_1_01.xml
Scanned items: 416206
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanRegistry=true|false

Die Registrierungsschlüssel auf Ihrem Computer scannen.

Standardwert: false

Beispiel:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom scanRegistry=true
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506073099_1_01.xml
Scanned items: 419060
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanMemory=true|false

Die in Ihrem Systempeicher ausgeführten Programme scannen.

Standardwert: false

Beispiel:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom scanMemory=true
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506072517_1_01.xml
Scanned items: 427016
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0

FileScan.OnDemand.RunScanTask custom scanMemory=true
```

smartScan=true|false

Scannen Sie nur neue und geänderte Dateien.

Standardwert: true

Beispiel:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom smartScan=false
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506070911_1_01.xml
Scanned items: 1614889
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanRootKits=true|false

Nach Rootkits und versteckten Objekten scannen, die diese Art von Software verwenden.

Standardwert: false

Beispiel:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom scanRootKits=true
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506070601_1_01.xml
Scanned items: 416548
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanKeyloggers=true|false

Nach Keylogger-Software scannen.

Standardwert: true

Beispiel:

```
FileScan.OnDemand.RunScanTask custom scanKeyloggers=false
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506069462_1_01.xml
Scanned items: 416845
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanPUA=true|false

Nach potenziell unerwünschten Anwendungen scannen (PUA).

Standardwert: false

Beispiel:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom scanPUA=true
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506068866_1_01.xml
Scanned items: 165522
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`scanArchives=true|false`

Nach infizierten Dateien in Archiven scannen.

Standardwert: `true`

Beispiel:

```
FileScan.OnDemand.RunScanTask custom scanArchives=false
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506069462_1_01.xml
Scanned items: 416845
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`extensionType=all|application|custom|none`

Dateien nach Dateierweiterung scannen: alle Dateien, nur ausführbare Dateien, nur Dateien mit den gewünschten Erweiterungen oder keine Dateien scannen.

Standardwert: `all`

Beispiel:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom extensionType=application
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506068866_1_01.xml
Scanned items: 165522
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`customExt="<string>"`

Mit dieser Option scannen Sie nur Dateien mit den gewünschten Erweiterungen. Trennen Sie dabei die einzelnen Erweiterungen in der Zeichenfolge mit einem senkrechten Strich. (z. B. "`|exe|ini|txt|`").

Diese Option ist nur in Kombination mit der Option `extensionType=custom` gültig.

Beispiel:

```

B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom path="c:\Program Files\WinRAR" extensionType=custom customExt="|dll|"
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506351027_1_01.xml
Scanned items: 6
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0

FileScan.OnDemand.RunScanTask custom path="c:\Program Files\WinRAR" extensionType=custom customExt="|dll|dat|"
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506351335_1_01.xml
Scanned items: 8
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
    
```

`lowPriority=true|false`

Die Aufgabe mit niedriger Priorität durchführen.

Standardwert: `false`

Beispiel:

```

B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom lowPriority=true
    
```

Diese Option stellen eine Alternative zu den in der BEST-Konsole verfügbaren Optionen dar. Weitere Informationen finden Sie unter [„Konfigurieren und Ausführen eines benutzerdefinierten Scans“](#) (S. 15).

6.2. Befehlszeilen-Fehlercodes

Das Befehlszeilentool gibt unter Umständen die folgenden Fehlercodes zurück:

| Fehlercode | Beschreibung |
|------------|--------------------------------|
| 0 | Befehl erfolgreich ausgeführt. |
| 87 | Ungültiger Parameter. |



| Fehlercode | Beschreibung |
|------------|--|
| 160 | Ungültige Argumente. |
| 1627 | Funktion fehlgeschlagen - beim Ausführen des Befehls ist ein Fehler aufgetreten. |



7. HILFE ERHALTEN

Sollten Sie Probleme oder Fragen zu Bitdefender Endpoint Security Tools haben, wenden Sie sich bitte an Ihren Netzwerkadministrator.

Klicken Sie mit der rechten Maustaste auf das Bitdefender Endpoint Security Tools-Symbol in der Task-Leiste und anschließend auf **Über**, um Produktinformationen und Kontaktdaten im **Über**-Fenster anzuzeigen.

Glossar

Adware

Adware wird häufig mit einer anderen Anwendung kombiniert, die kostenlos ist, solange der Nutzer die Adware akzeptiert. Adware-Anwendungen werden in der Regel installiert, nachdem der Nutzer einer Lizenzvereinbarung zugestimmt hat. In der Lizenzvereinbarung wird auch der Zweck der Anwendung genannt, und somit liegt keine Rechtswidrigkeit vor.

Allerdings können Popup-Anzeigen mit der Zeit sehr lästig werden und in manchen Fällen die Systemperformance beeinträchtigen. Zudem kann aufgrund der Daten, die manche dieser Programme sammeln, die Privatsphäre von Nutzern verletzt werden, die sich über die Bedingungen in der Lizenzvereinbarung nicht völlig im Klaren waren.

Archiv

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

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

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.

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.

Boot-Sektor:

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

Bootkit

Ein Bootkit ist ein Schadprogramm, das den Master Boot Record (MBR), den Volume Boot Record oder den Boot-Sektor infizieren kann. Ein Bootkit bleibt auch nach einem Neustart des Systems aktiv.

Bootvirus

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

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. Andererseits 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.

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.

Durchsuchen

Kurzform für Web-Browser, ein Programm, mit dem Internetseiten aufgerufen und angezeigt werden können.

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.

Exploit

Als Exploit wird zum einen eine Methode bezeichnet, mit der Unbefugte auf einen Computer zugreifen, zum anderen eine Schwachstelle in einem System, über die das System angegriffen werden kann.

Fehlalarm

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

Gezielte Angriffe

Cyber-Angriffe, die es hauptsächlich auf finanzielle Vorteile oder die Erschütterung eines guten Rufs abgesehen haben. Opfer können Einzelpersonen, Unternehmen, eine Software oder ein System sein. In jedem Fall wird das Opfer vor dem Angriff genauestens studiert. Diese Art von Angriffen wird über einen langen Zeitraum hinweg und in verschiedenen Phasen durchgeführt, wobei oft mehr als ein Einfallstor ausgenutzt wird. Sie werden kaum bemerkt, und wenn doch, dann meist erst, wenn es schon zu spät ist.

Grayware

Eine Klasse von Software-Anwendungen irgendwo zwischen legitimer Software und Malware. Sie ist zwar nicht so unmittelbar schädlich wie Malware, die die Systemfunktion direkt beeinträchtigt, ihr Verhalten ist aber dennoch beunruhigend und kann zu unerwünschten Situationen führen. Daten können gestohlen, Identitäten missbraucht und Werbung eingeblendet werden. Die verbreitetsten Arten von Grayware sind [Spyware](#) und [Adware](#).

Heuristik

Eine Methode, um neue Viren zu identifizieren. Diese Scan-Methode benötigt keine spezifischen Virussignaturen. Der Vorteil eines heuristischen Scans ist, dass man nicht von einer neuen Variante eines alten Virus 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.

IP

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

Keylogger

Ein Keylogger ist eine Anwendung, die alles aufzeichnet, was Sie tippen.

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 bössartiger Absicht eingesetzt (um beispielsweise private Daten wie Benutzernamen oder Passwörter zu sammeln).

Logdatei (Berichtsdatei)

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

Makrovirus

Eine Virusform, 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.

Malware

Malware ist der Sammelbegriff für alle Software-Arten, die darauf ausgelegt sind, Schaden zu verursachen - das Wort setzt sich zusammen aus den englischen Begriffen malicious und software, also bössartige Software. Der Begriff hat sich noch nicht vollständig durchgesetzt, wird aber immer häufiger als Oberbegriff gebraucht, wenn von Viren, Trojanern, Würmern und Malicious Mobile Code die Rede ist.

Malware-Scan-Ressourcenkonflikt

Eine intensive Beanspruchung von Systemressourcen, die auftritt, wenn Virenschutz-Software gleichzeitig mehrere virtuelle Maschinen auf einem einzigen physischen Host scannt.

Malware-Signatur

Malware-Signaturen sind Codebruchstücke, die aus aktuellen Malware-Beispielen extrahiert werden. Diese werden von Antiviren-Programmen zum Musterabgleich und zur Aufspürung von Malware verwendet. Signaturen werden auch genutzt, um den Malware-Code aus infizierten Dateien zu entfernen.

Die Bitdefender Malware-Signatur-Datenbank ist eine Sammlung von stündlich durch Bitdefender-Mitarbeiter upgedateten Malware-Signaturen.

Nicht heuristisch

Diese Scan-Methode beruht auf spezifischen Virussignaturen. Der Vorteil eines nicht-heuristischen Scans ist, dass er nicht von einem Scheinvirus getäuscht werden kann und so Fehlalarme verhindert.

Passwort-Stehler

Ein Passwort-Stehler sammelt Daten wie Benutzernamen und Passwörter für Konten. Die gestohlenen Zugangsdaten werden dann zu kriminellen Zwecken genutzt.

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.

Polymorpher Virus

Ein Virus, der seine Form mit jeder Datei, die er infiziert, ändert. Da diese Viren kein beständiges binäres Muster haben, sind sie sehr schwer zu erkennen.

Ransomware

Eine Schadsoftware, die Ihren Computer sperrt oder Ihnen den Zugriff auf Ihre Dateien und Anwendungen verwehrt. Ransomware verlangt die Zahlung eines bestimmten Betrags (Lösegeldzahlung) als Gegenleistung für einen Entschlüsselungscode, der den Zugang zum Computer und Ihren Dateien wieder freigibt.

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, Malware zu verbergen oder unbemerkt einen Eindringling einzuschleusen. In Kombination mit Malware stellen sie 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 Schnittstellenummer 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.

Einem Trojanischen 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.

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 bössartiges Programm, das sich als eine legitime Anwendung ausgibt. Im Unterschied zu Viren vervielfältigen sich die Trojaner (auch "trojanische Pferde" genannt) nicht, aber sie können ebenso schädlich sein. Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Viren 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 schenken. 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 ein eigenes Update-Modul, das die manuelle oder automatische Suche nach Updates ermöglicht.

Verdächtige Dateien und Netzwerkverkehr

Verdächtige Dateien sind solche mit einer zweifelhaften Reputation. Diese Einstufung basiert auf mehreren Faktoren, darunter: Vorhandensein der digitalen Signatur, Anzahl der Vorkommen in Computernetzwerken, verwendeter Packer, usw. Netzwerkverkehr gilt als verdächtig, wenn er vom Muster abweicht. Zum Beispiel bei unzuverlässiger Quelle, Verbindungsanfragen an ungewöhnliche Ports, hohe Bandbreitennutzung, zufällig scheinende Verbindungszeiten, usw.

Virus

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 Viren können sich auch selbst vervielfältigen. Alle Computerviren wurden von Menschen programmiert. Ein Virus, das sich immer wieder vervielfältigen kann, ist sehr einfach zu programmieren. Sogar ein solch einfacher Virus kann gefährlich sein, da er im Handumdrehen sämtlichen Arbeitsspeicher belegen und so das System lahmlegen kann. Noch gefährlicher sind Viren, die sich über Netzwerke selbst weiterversenden und Sicherheitssysteme umgehen.

Windows-Downloader

Es ist ein generischer Name für ein Programm, dessen primäre Funktion darin besteht, Inhalte zu unerwünschten oder schädlichen Zwecken herunterzuladen.

Wurm

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